AFRL-RI-RS-TR-2013-071

CYBER FUNDAMENTAL EXERCISES

MARCH 2013

INTERIM TECHNICAL REPORT

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

REPORT DOCUMENTATION PAGE

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MARCH 2013	INTERIM TECHNICAL REPORT	Jan 2010 – Aug 2010

4. TITLE AND SUBTITLE

CYBER FUNDAMENTAL EXERCISES

5a. CONTRACT NUMBER	IN-HOUSE
5b. GRANT NUMBER	N/A
5c. PROGRAM ELEMENT NUMBER	62788F

6. AUTHOR(S)

Sonja Glumich

5d. PROJECT NUMBER	GAIH
5e. TASK NUMBER	CY
5f. WORK UNIT NUMBER	BR

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RIGA
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2013-071

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. PA# 88ABW-2011-3062
Date Cleared: 31 MAY 2011

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The author utilized the exercises with undergraduate and graduate students studying computer science, computer engineering, electrical engineering, physics, and mathematics. The intent of these exercises is to provide enough information to enable students to complete the exercises independently of an instructor. At the time of writing this introduction, with the exception of the Windows operating system, the software applications referenced in the exercises are free to download.

15. SUBJECT TERMS

Cyber, Training, Fundamentals, Education

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	90	**E. PAUL RATAZZI**
U	U	U			**19b. TELEPONE NUMBER** *(Include area code)* N/A

TABLE OF CONTENTS

iv

Introduction

The intent of these exercises is to provide enough information to enable students to complete the exercises independently of an instructor. At the time of writing this introduction, with the exception of the Windows operating system, the software applications referenced in the exercises are free to download. The author utilized the exercises with undergraduate and graduate students studying computer science, computer engineering, electrical engineering, physics, and mathematics.

Cyber Fundamentals #1: VMware and Ubuntu Linux

1. Introduction

Linux is a (mostly) free and open-source alternative to the Windows and Macintosh Operating Systems (OS). There are many different distributions of Linux, including Ubuntu, Red Hat, Fedora, Mandriva, and Slackware. See the website http://distrowatch.com/ for additional distributions. Ubuntu is very popular because it is easy to use and works "out of the box" with most hardware.

VMware Server is a free program used to create virtual environments. For example, VMware Server enables users to run a Linux virtual environment on a Windows host, a Windows virtual environment on a Linux host, a Windows XP virtual environment on Windows Vista host, etc.. This brief activity introduces you to VMware Server and the Ubuntu Operating System (OS). The goal of this exercise is to create a virtual Ubuntu image and execute a few Linux commands.

Linux image running in VMware

1.1 Objectives

- Create an image with VMware

- Install the Ubuntu Linux OS

- Execute basic Linux commands

1.2 Materials
- Computer with access to an account with administrative rights

- VMware Server

- Ubuntu OS iso file

1.3 Assumptions
- The instructions provided for this activity were tested using a Windows Vista physical machine and an Ubuntu 9.04 image. Instructions may vary for other OS.

- The student has administrative access to their system and possesses the right to install programs

- The student's computer has Internet access

- Note: VMware Server on Windows XP requires an Internet connection to work!
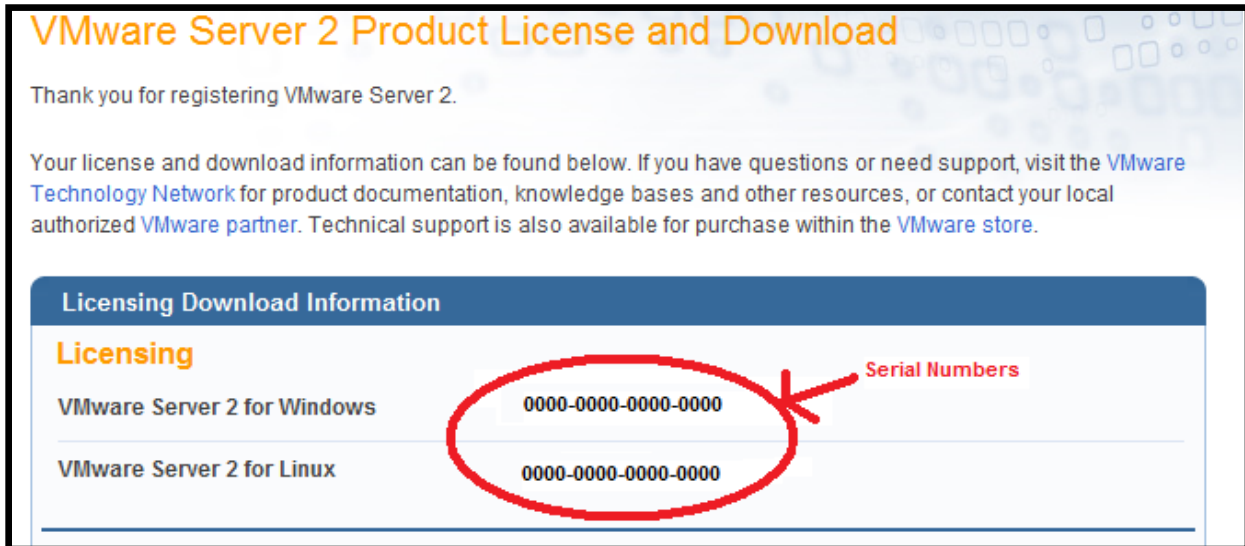
1.4 Note on MD5 Checksums
- The MD5 checksum (or hash) of a file serves as a unique identifier for that file. If one bit is changed in a file, its MD5sum changes. The MD5sum of a file is useful for verifying the file downloaded correctly.

- See https://help.ubuntu.com/community/HowToMD5SUM for instructions.

2. Download and Install VMware

2.1 Download

- Download the latest version of VMware Server for your computer's OS from http://www.vmware.com/products/server/

- You must register to receive a serial number. Please note the serial number as provided by the VMware website. You will need it during installation.
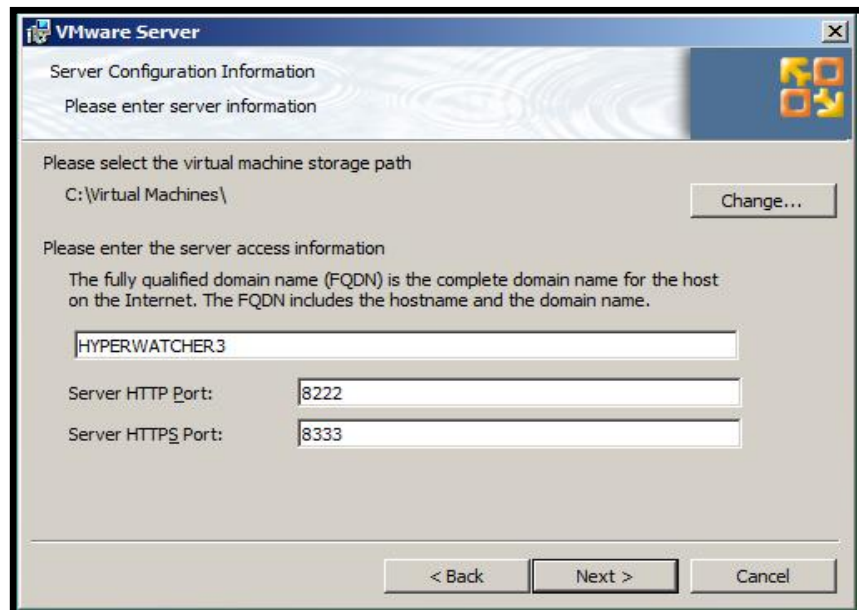
2.2 Install

- Start the installation by double clicking the downloaded file and accept the license agreement
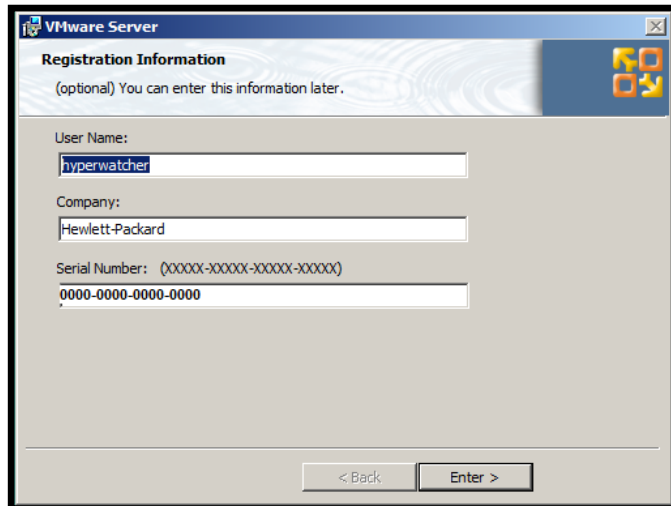
- Accept the default destination folder

- On "Server Configuration Information" make sure there are no port conflicts (no other applications already using the ports). The default ports 8222 and 8333 should be fine in most cases. Select *Next* to continue.

- Select desired shortcuts

- On next screen click "Install"

- After installation, enter the serial number from the VMware website

- Restart the system

3. Download Ubuntu OS .iso File

- Download the latest Ubuntu .iso file from http://www.ubuntu.com/GetUbuntu/download

- Find a list of Ubuntu MD5sums to verify the file downloaded correctly at:
  https://help.ubuntu.com/community/UbuntuHashes

- Ubuntu is license-free

4. Run VMware
4.1 Start VMware

- Click on Desktop icon OR

- Go to *Start > All Programs > VMware > VMware Server > VMware Server Home Page*

4.2 If (Your Browser == Firefox)

If you use Firefox and receive the error "<computername>:8333 uses an invalid security certificate. The certificate is not trusted because it is self signed. (Error code: sec_error_untrusted_issuer)" follow the instructions in the subsequent sub-bullets.

- o Go to *Tools > Options > Advanced Tab > Encryption Tab > View Certificates*

- o Click on the *Server Tab > Add Exception*
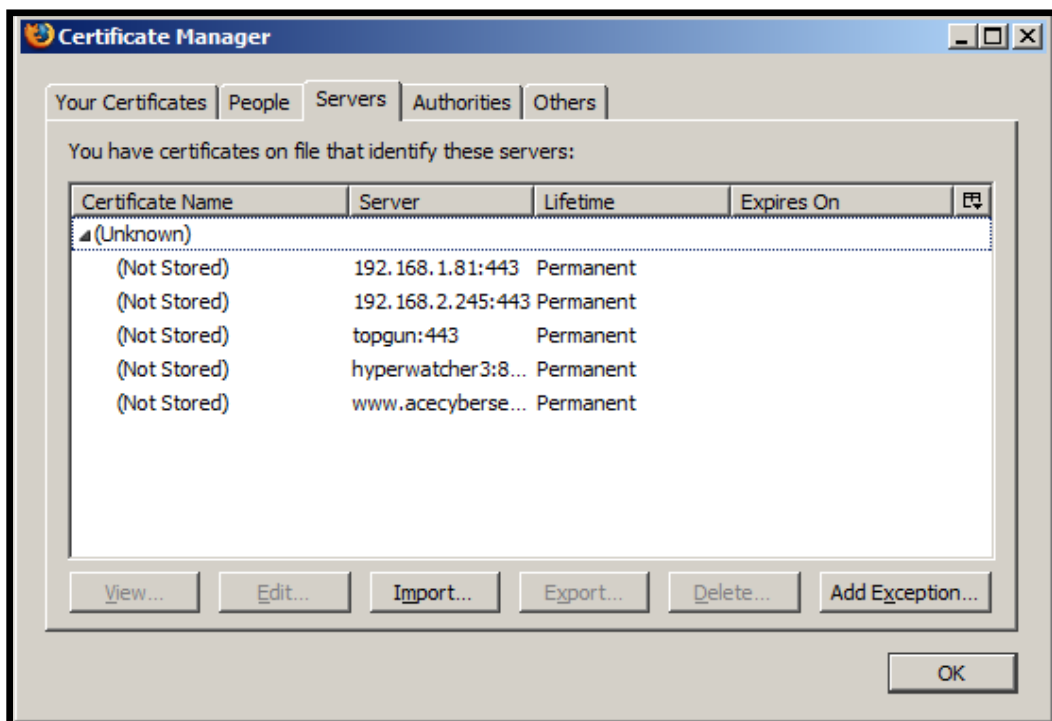
- o Type in the website (something like https://<computername>:8333)

o Select Get Certificate > Confirm Security Exception
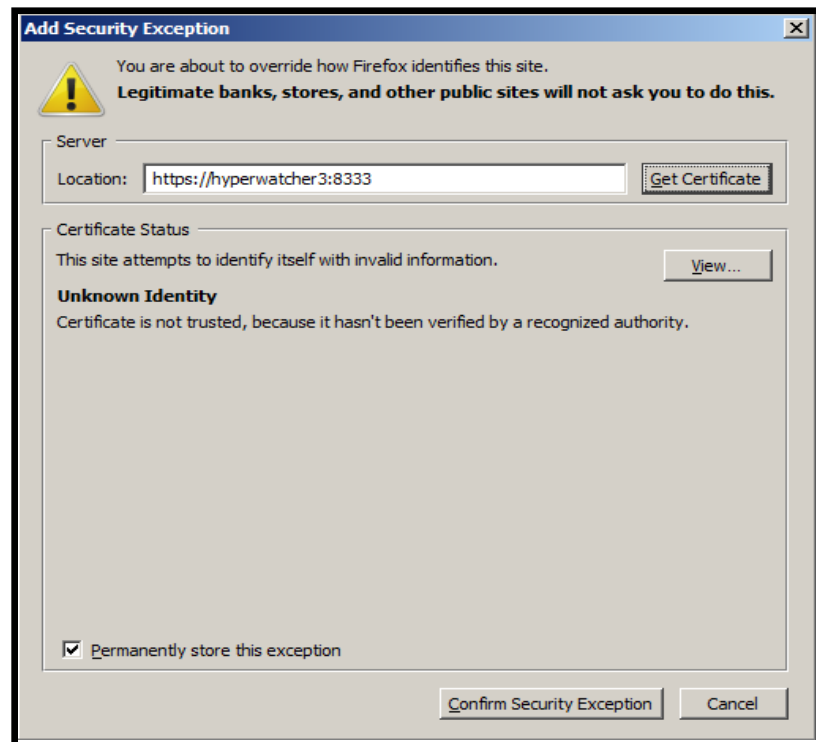
o Select OK

4.3 If (Your Browser == Internet Explorer (IE))

If you use IE and receive the error "There is a problem with this website's security certificate", take the following steps:

- Click **Continue to this website**

- Confirm by clicking Y*es* in the pop-up box

- Restart VMServer to get the login screen. Login with the computer OS (Vista login for example) user name and password.
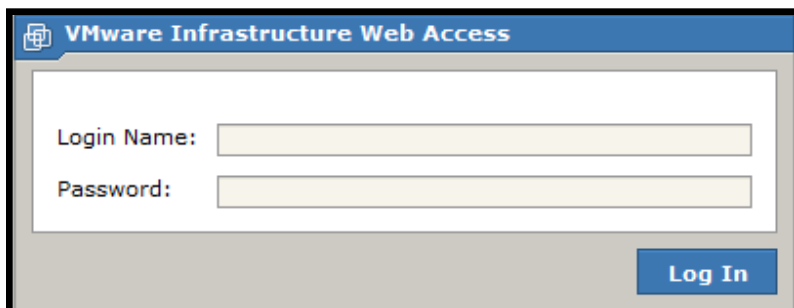
- Upon login, you'll a screen similar to the screenshot below
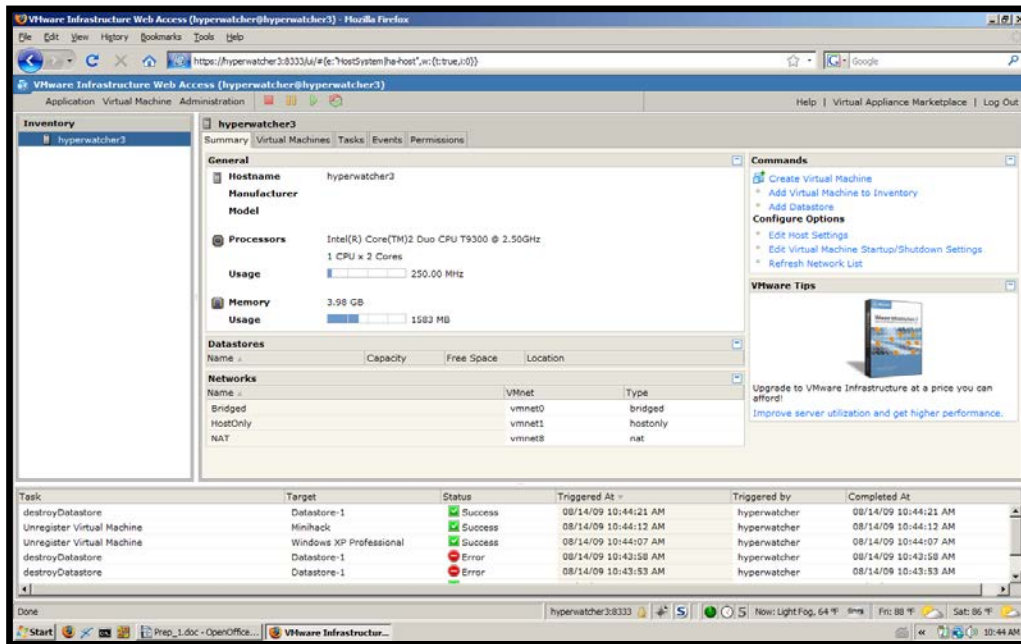
4.4 Create a Virtual Machine
- **Create New Directory:** Through Windows Explorer (not using VMware), create a new directory to store your virtual machines. I created the directory C:\my_virt_machines.
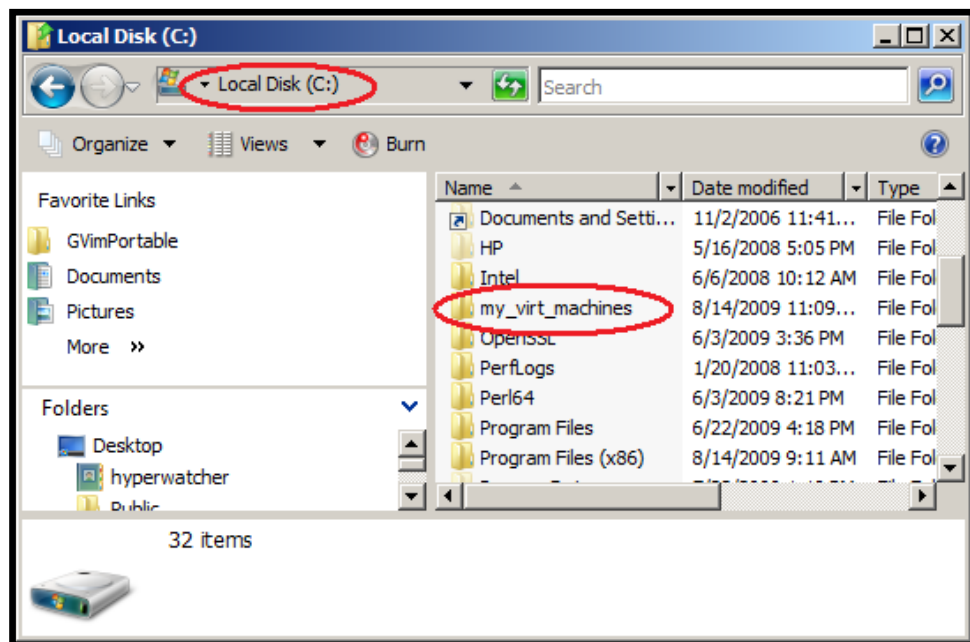
- **Move Ubuntu .iso file to New Directory:** Move the Ubuntu iso file downloaded previously to the new directory. For example location of the iso file in the image below is C:\my_virt_machines\ubuntu-9.04-desktop-i386.iso.
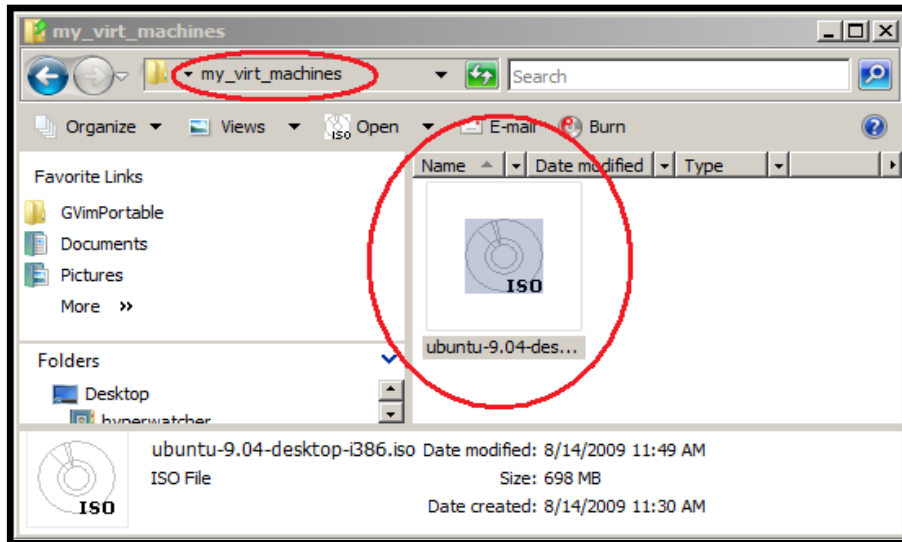
- **Give VMware the Directory Location:** Select *Add Datastore* from the upper right hand side of the screen. (A datastore is the directory that holds your VMware machine files.)

- Add the name and path of the directory you created using Windows Explorer and select **OK**.
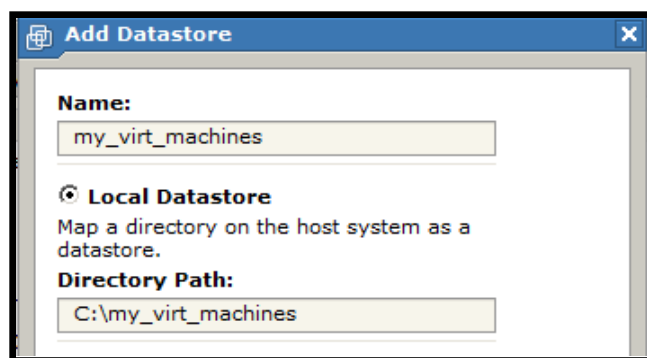
- Select *Create Virtual Machine* from the upper right hand side of the screen
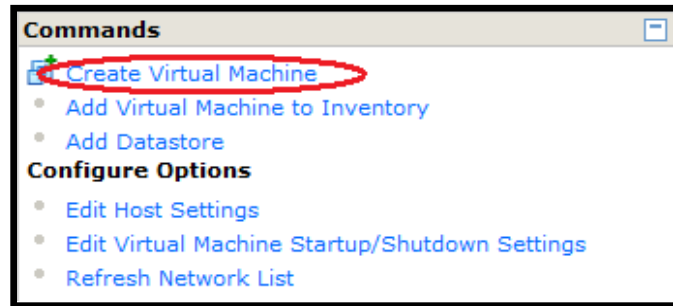
- Name your virtual machine *<your first name>.<your last name>.* Note the new datastore *my_virt_machines* is selected. Select *Next.*

- Select Linux OS and Ubuntu Linux (32-bit or 64-bit depending on the version of Ubuntu you downloaded earlier – most likely you chose 32-bit). Select *Next*.

- Keep the defaults for **Memory and Processors** and select *Next*

- Keep the default for **Hard Disk** and select *Next*

- Keep the default for **Properties** and select *Next*

- Keep the default for **Add a Network Adaptor** and select *Next*

- Keep the default for **Properties** and select *Next*

- For CD/DVD Drive select *Use an Iso Image* and select *Next*
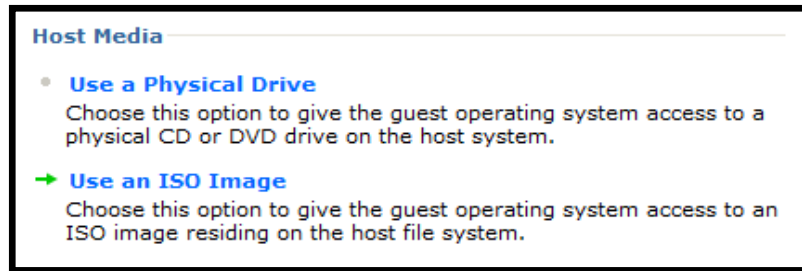
- Select the Ubuntu iso you added to your datastore and select *OK*
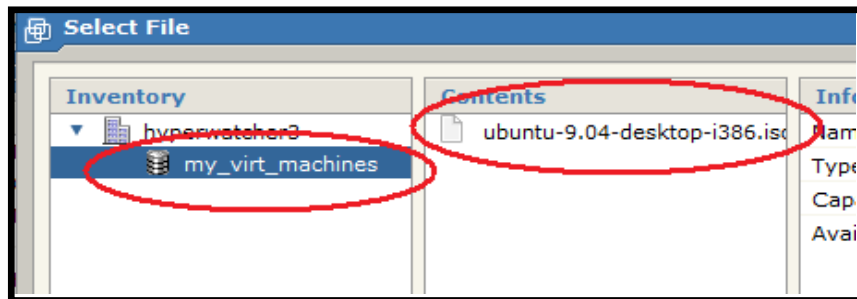
- Keep the default for **Properties** and select *Next*

- Select *Don't Add a Floppy Drive* and select *Next*

- Keep the default for *USB Controller* (to add a USB Controller) and select *Next*

- Select *Finish*

Power on the Image and Install the Ubuntu OS
- If you successfully created a new image, it will appear the upper left-hand corner of the screen
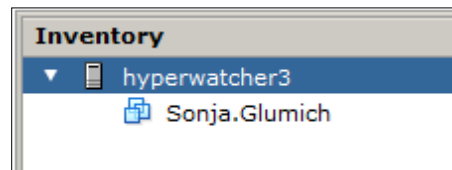
- Select and highlight the image name (Sonja.Glumich) and select *Play*
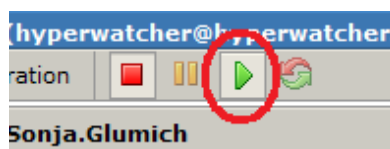
- Select the *Console* tab and click the screen to open a new window
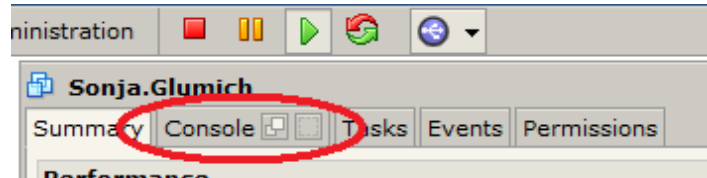
- If installation does not start automatically, click inside the brown Ubuntu window to transfer control of the mouse to the image and select *install*. To transfer mouse control back to the host computer, press ctrl-alt together.
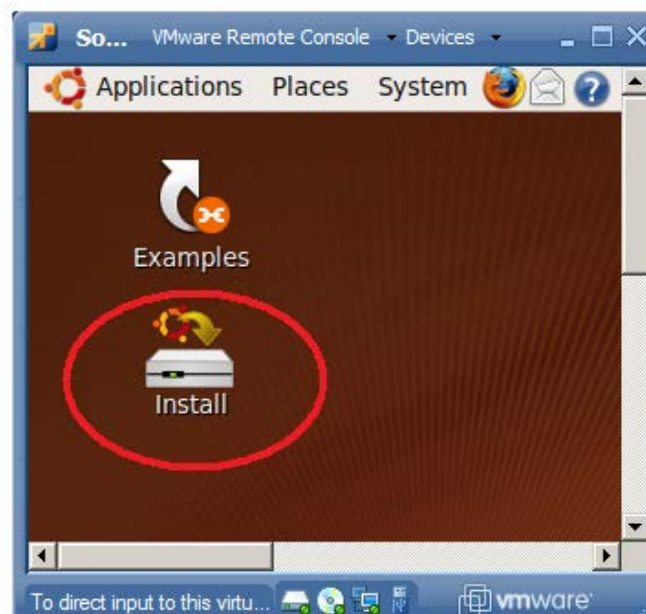
- The Ubuntu installation is very straightforward.
  - Select all defaults
  - Specify a user name of *ace*
  - Specify a password of *ilikeace*
  - Specify a computer name *ace*

- After installation completes, restart the image.

- Log in with your user name (ace) and password (ilikeace). Please note that if you decide to use your image for anything important/personal beyond the ACE exercises it is recommended you change the password to something more secure.

5. Execute a Linux Command

- Open a terminal by selecting *Applications > Accessories > Terminal*
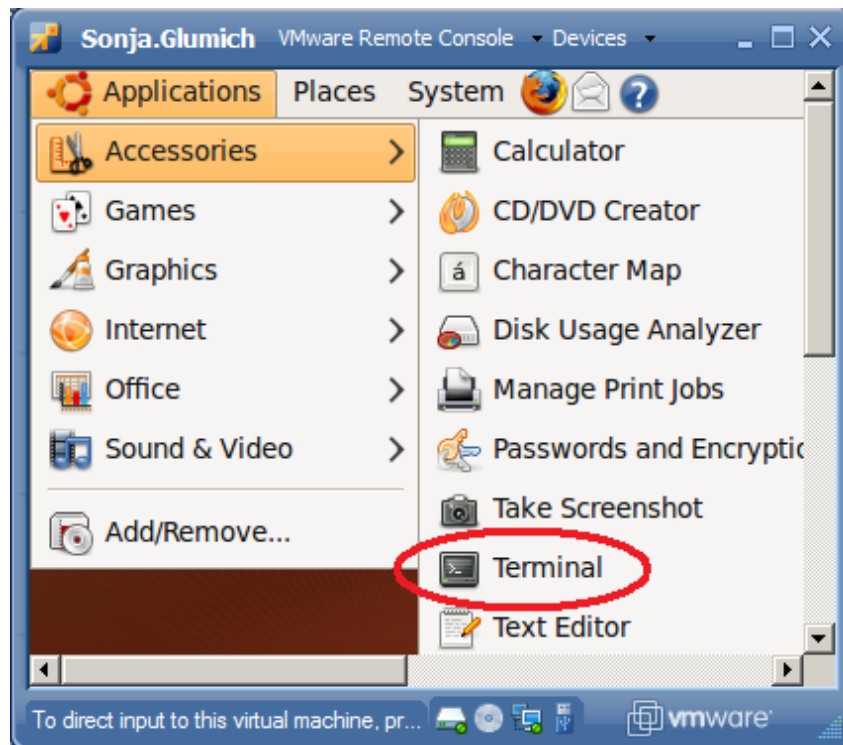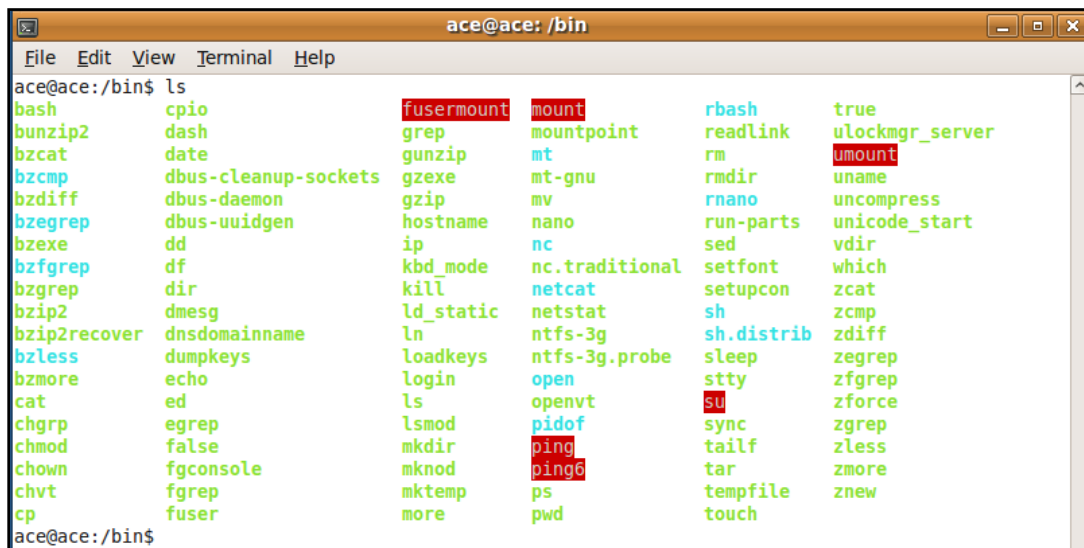
- Type the following commands into the command prompt
  - *whoami* (list the user name you are currently using)
  - *man whoami* (the man or "manual" command gives you information about topics commands, etc.)
  - *whoami - -help* (adding "dash dash help" is another way..don't put a space between the dashes, only added for clarity)
  - *apropos whoami* (finally apropos is yet another way to get help)
  - *perl -h* (adding a single dash followed by h is yet another way...but it doesn't work with whoami so I used perl as an example)
  - *ls* (list files in directory)
  - *pwd* (list the present working directory)
  - *sudo -s* (enter your password when prompted – this gives you administrative or root access – required for shutting down the system (next command))
  - *shutdown -h now* (powers off the system)
  - For more information on commands – visit ***https://help.ubuntu.com/7.04/basic-commands/C/***

Cyber Fundamentals #2: Review of the Linux File System and Linux Commands

1. Introduction

Becoming adept at using the Linux OS requires gaining familiarity with the Linux file system, file permissions, and a base set of Linux commands. In this activity, you'll study how the Linux file system is organized and practice utilizing common Linux commands.

The /bin (binary) directory contains executable commands for all users

1.1 Objectives

- Describe the purpose of the /bin, /sbin, /etc, /var/log, /home, /proc, /root, /dev, /tmp, and /lib directories

- Describe the purpose of the /etc/shadow and /etc/passwd files

- Utilize a common set of Linux commands including ls, cat, and find

- Understand and manipulate file permissions, including rwx, binary, and octal formats

- Change the group and owner of a file

1.2 Materials

- Windows computer with access to an account with administrative rights

- VMware Server

- Ubuntu OS iso file

1.3 Assumptions

- The provided instructions were tested on an Ubuntu Jaunty Jackalope image running on a Windows Vista physical machine. Instructions may vary for other OS.

- The student has administrative access to their system and possesses the right to install programs

- The student's computer has Internet access

2. Directories

2.1 /

The / directory or root directory is the mother of all Linux directories, containing all of the other directories and files. From a terminal users can type *cd /* to move to the root directory.

2.2 /home

The home directory stores user-specific directories and files. For instance, during the Ubuntu installation process, you created an account named ace. Creating the ace account through the GUI or with the adduser command automatically creates a directory named /home/ace to store ace's personal files. This directory is known as ace's home directory, as specified in the /etc/shadow file (see section 2.6). From a terminal users can type *cd ~* to move to the current user's home directory.

2.3 /root

The /root directory is the home directory for the root account. (Like /home/ace is the home directory for the ace account.)
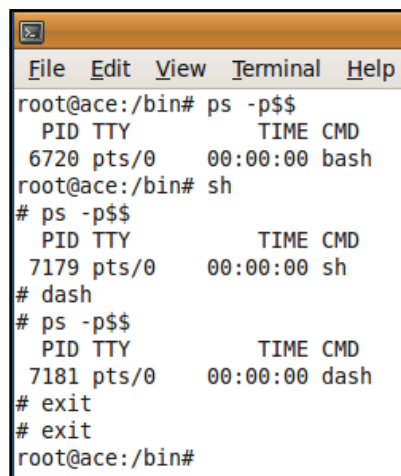
2.4 /bin

2.4.1 Purpose

The term *bin* stands for binaries or executable files. The /bin directory typically holds commands executable by any user. (e.g. ls, pwd, cat, rm)

2.4.2 Linux Shells

The /bin directory also contains shell binaries such as /bin/bash and /bin/sh. A shell is a special executable that starts an interactive, text-based window and enables users to enter commands. The shell executes the commands and displays the output back to the user. There are different shells (bash, sh, dash, and others) that offer slightly different functionality and sets of commands. By default Ubuntu assigns users the /bin/bash shell. To determine your current shell in a terminal, type *ps -p$$*. Try the commands in the screenshot below:


```
File  Edit  View  Terminal  Help
root@ace:/bin# ps -p$$
  PID TTY          TIME CMD
 6720 pts/0    00:00:00 bash
root@ace:/bin# sh
# ps -p$$
  PID TTY          TIME CMD
 7179 pts/0    00:00:00 sh
# dash
# ps -p$$
  PID TTY          TIME CMD
 7181 pts/0    00:00:00 dash
# exit
# exit
root@ace:/bin#
```
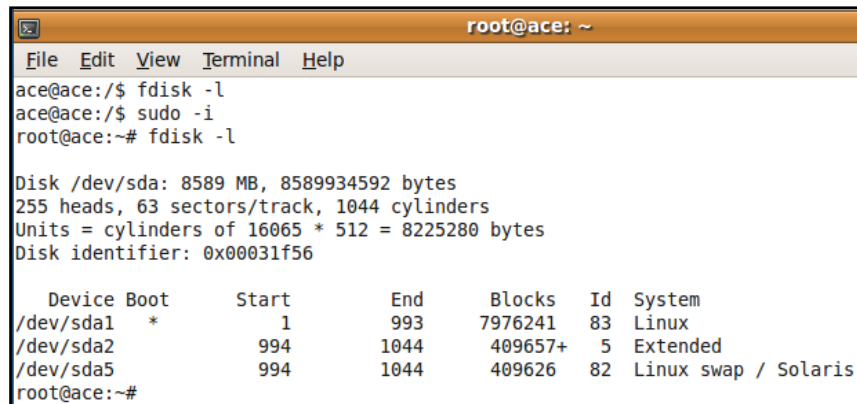
Experimenting with shells

Note that user in the screenshot example begins in a bash shell, starts a sh shell, and then starts a dash shell. To return to the bash shell, the user types exit (return to sh) and types exit again (return to bash).

2.5 /sbin

The term *sbin* stands for *system binaries* which are files executed by the system or privileged users. Try the fdisk command which resides in /sbin – first as *ace*, then with *root* privileges:

```
root@ace: ~
File  Edit  View  Terminal  Help
ace@ace:/$ fdisk -l
ace@ace:/$ sudo -i
root@ace:~# fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00031f56

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1         993     7976241   83  Linux
/dev/sda2             994        1044      409657+    5  Extended
/dev/sda5             994        1044      409626    82  Linux swap / Solaris
root@ace:~#
```
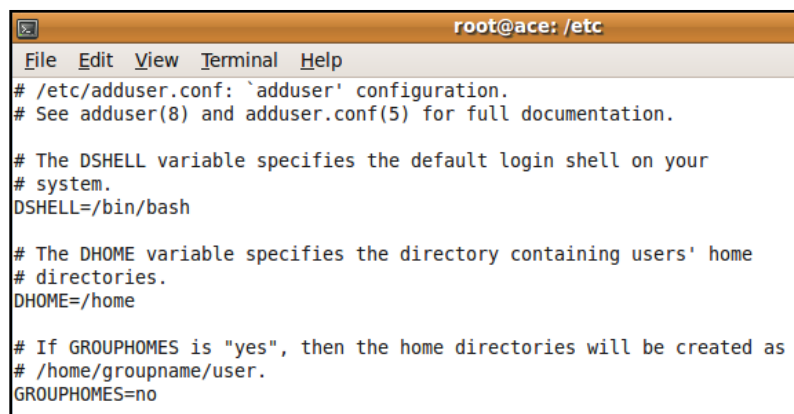
The fdisk command

With ace account privileges, the command executes without an error, but does not display any results. With root privileges it lists information about the partition table.

2.6 /etc

2.6.1 Introduction

The /etc directory holds configuration files for the operating system and applications. For example, the /etc/addusers.conf file specifies options for the adduser command.

```
root@ace: /etc
File  Edit  View  Terminal  Help
# /etc/adduser.conf: `adduser' configuration.
# See adduser(8) and adduser.conf(5) for full documentation.

# The DSHELL variable specifies the default login shell on your
# system.
DSHELL=/bin/bash

# The DHOME variable specifies the directory containing users' home
# directories.
DHOME=/home

# If GROUPHOMES is "yes", then the home directories will be created as
# /home/groupname/user.
GROUPHOMES=no
```

/etc/adduser.conf

The adduser.conf file allows system administrators to specify the default home directory for new users. The default is /home/<user>, but it could be changed to another existing directory.

2.6.2 /etc/passwd and /etc/shadow
The /etc/shadow file didn't exist on early Linux distributions. Originally only root could access the /etc/passwd file, which stored user names, user configuration information, and passwords. However, when common programs such as ls running under reduced privileges needed access to user names, passwords were moved to the shadow file. Now almost any account can view the passwd file, but only root or administrators can view the shadow file. Please open a terminal and execute the commands below to view the /etc/passwd and /etc/shadow files. Do not type the comments, which is the text preceded by two forward slashes *//*.

- Open a terminal
- *cd /etc*   //Move to the etc directory
- *ls*   //List files
- *cat passwd*   //View the /etc/passwd file
- *cat shadow*   //Error - regular user cannot view the /etc/shadow file
- *sudo -s*   //Escalate to root privileges
- *cat /etc/shadow*   //View the /etc/shadow file

Sample /etc/passwd entry for the ace account:

ace : x : 1004 : 1004 : , , , : /home/ace : /bin/bash
- **ace** - username
- **x** – indicates the password hash stored in /etc/shadow
- **1004** - user id
- **1004** - group id
- **„,** - place to list user ID info (name, phone number, etc)
- **/home/ace** - home directory
- **/bin/bash** - user's default shell

Sample /etc/shadow entry for the ace account:

ace : 6eaG47PNn$HW.J8bMbRmEiki7E5K8QwW2U1aWkJzH80AsGTDqoS6sm5EP.JLjw 7r03PrgXuyvlnqetqa4TvCkuQ.ybsCZ10 : 14524 : 0 : 99999 : 7 :::
a) **ace** – Username
b) **:** and **$** – Delineators
c) **6** – Indicates algorithm (SHA-512 in this case)
d) **$** – Delineator
e) *eaG47PNn* **–** Password salt
f) **$** – Delineator
g) **HW...Z10** – SHA hash of password
h) **14524** – Number of days since (Jan 1970) the password was last changed
i) **0** – Number of days before password can be changed (0 means can change any time)
j) **99999** – Number of days until required to change password
k) **7** – Number of days to warn user of password expiration
l) **:::** – Number of days after which password is disabled, Number of days since Jan 1, 1970 that account has been disabled, Reserved field for future use

2.7 /lib

The /lib or library directory holds shared libraries used by the system and its applications. Library files are typically named <library name>.so.<version number>. This directory also holds kernel modules, which if loaded add functionality to the base Linux kernel.

2.8 /dev
The /dev or device directory contains special files for devices such as the hard drive, printers, external drives, and ports.
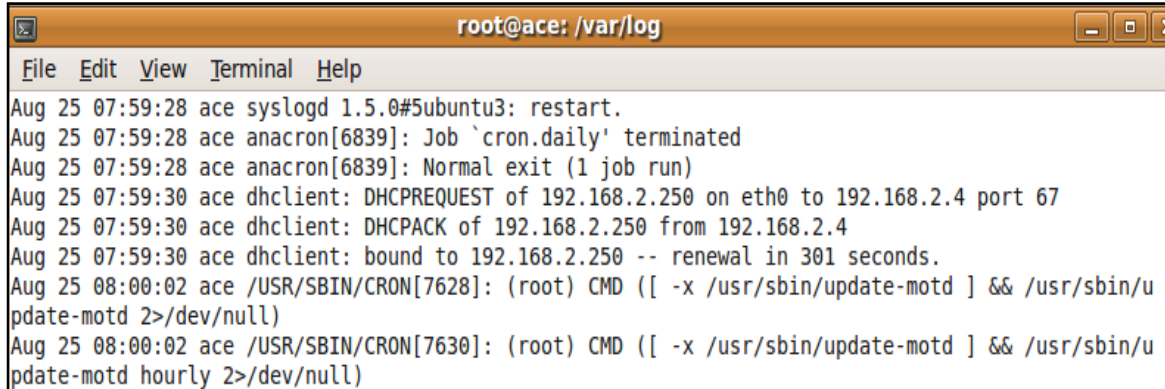
2.9 /proc
The /proc directory holds operating system state information on running processes and hardware. It is a virtual file system stored in memory (volatile). Directories named after process ids store information about processes.

2.10 /tmp
The /tmp or temporary directory is a place to store temporary files. The system typically deletes temporary files upon every boot-up.

2.11 /var/log
The /var/log directory holds the log files for the system and applications, including web servers, ftp servers, etc. Below see *syslog* (system log) output showing a restart, the system requesting an IP address, and some commands executed as the root account.


```
root@ace: /var/log

File  Edit  View  Terminal  Help
Aug 25 07:59:28 ace syslogd 1.5.0#5ubuntu3: restart.
Aug 25 07:59:28 ace anacron[6839]: Job `cron.daily' terminated
Aug 25 07:59:28 ace anacron[6839]: Normal exit (1 job run)
Aug 25 07:59:30 ace dhclient: DHCPREQUEST of 192.168.2.250 on eth0 to 192.168.2.4 port 67
Aug 25 07:59:30 ace dhclient: DHCPACK of 192.168.2.250 from 192.168.2.4
Aug 25 07:59:30 ace dhclient: bound to 192.168.2.250 -- renewal in 301 seconds.
Aug 25 08:00:02 ace /USR/SBIN/CRON[7628]: (root) CMD ([ -x /usr/sbin/update-motd ] && /usr/sbin/u
pdate-motd 2>/dev/null)
Aug 25 08:00:02 ace /USR/SBIN/CRON[7630]: (root) CMD ([ -x /usr/sbin/update-motd ] && /usr/sbin/u
pdate-motd hourly 2>/dev/null)
```

The syslog file

3. Twenty-three Useful Linux Commands

This section covers a set of twenty-three Linux commands. *Switches* are command modifiers that often take the syntax of a dash followed by a letter (-h) or two dashes followed by a word (--help). Open a terminal and type the commands in order as listed. Do not type the comments, which is the text preceded by two forward slashes *//*.

3.1 ls (List Files)

- *ls* //List files
- *ls -a* //List all files including hidden files (file name prefaced by a dot)
- *ls -l* //List files in long format
- *ls -al* //List all files in long format
- *ls -il* //List the index number or inode of each file in long format
- *ls --help* //To get more information about the ls or many other commands
- *man ls* //To get more information about the ls or many other commands
- *apropos ls* //To get more information about the ls or many other commands

3.2 cd (Change Directory)

- *cd /* //Move to the root directory
- *cd /home/ace* //Move to the home directory of user ace
- *cd ..* //Move up a directory (to /home)
- *cd ..* //Move up a directory (to /)
- *cd ~* //Move to the home directory of the current user ace

3.3 pwd (Print Working Directory)

- *cd /* //Move to the root directory
- *pwd* //List the current working directory
- *cd ~* //Move to the home directory of the current user ace
- *pwd* //List the current working directory
- *cd ..* //Move up a directory
- *pwd* //List the current working directory
- *cd /home/ace* //Move to the home directory of user ace
- *pwd* //List the current working directory

3.4 touch (Create a file, Change the file timestamp)

- *cd ~/Desktop* //Move to the Desktop of the current user ace
- *touch test.doc* //Create an empty file
- *touch test1.doc test2.doc* //Create two empty files
- *touch -d '1 May 2005 10:22' test.doc* //Change the last access time on a file to the time specified
- *ls -al* //Verify the time change on file test.doc

3.5 cat (Display the contents of a file) and tac (Display backwards)

- *cd ~/Desktop* //Move to the Desktop of the current user ace
- *touch test.doc* //Create an empty file
- *cat test.doc* //Since the file is empty, displays nothing
- Move to the desktop GUI and double-click on test.doc to open it in an editor.
- Add some text and save the changes.
- Return to the terminal
- *cat test.doc* //Displays contents of test.doc
- *tac text.doc* //Displays contents of test.doc last line first and first line last

3.6 echo (Echo back text or variable values ($) to the terminal)
- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *echo Hello World!*   //Echos "Hello World" back to you on the terminal
- *echo Hello World! > hello.txt*   //Writes "Hello World" into a new file called hello.txt
- *echo $PATH*   //Echo the current user's path (lists the directories where the system automatically looks for commands)

3.7 cp (Copy a file)
- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *echo hi > star.doc*   //Create file named star.doc containing "hi"
- *cat star.doc*   //Verify text "hi" is in star.doc
- *cp star.doc venus.doc*   //Copy star.doc to new file venus.doc
- *cat venus.doc*   //Verify text "hi" is in venus.doc

3.8 rm (Remove a file)
- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *ls*   //List files
- *rm star.doc*   //Remove (delete) star.doc
- *rm test**   //Remove all files starting with test. The * is a wild card.

3.9 mkdir, rmdir, and rm -rf (Make and remove directories)
- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *mkdir emptydir*   //Make an empty directory called emptydir
- *mkdir clowndir*   //Make a directory called clowndir
- *cd clowndir*   //Move to directory clowndir
- *touch bozo.txt*   //Create an empty file in clowndir called bozo.txt
- *echo big nose > curly.txt*   //Create a file curly.txt containing "big nose" in clowndir
- *cd ..*   //Move up one level to Desktop
- *rmdir emptydir*   //Delete the emptydir directory
- *rmdir clowndir*   //Try to remove clowndir, but get error due to contents
- *rm -rf clowndir*   //Recursively remove clowndir and its contents (be very careful using the rm -rf command!)

3.10 su (Switch user)
- *sudo -s*   //Switch to root access
- *su ace*   //Switch back to ace user account

3.11 whoami (List current user name)
- *whoami*   //List current user ace
- *sudo -s*   //Switch to root access
- *whoami*   //List current user root
- *su ace*   //Switch back to ace user account

3.12 nano, gedit (Text editors)

- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *nano nano.txt*   //Open a new file for writing in the terminal text editor nano
- Write some text into nano.txt
- Press **control-X** to exit the program
- Type **Y** and hit **enter** to confirm exit and save
- *gedit gedit.txt&*   //Open a new file for writing in the GUI text editor gedit
  //Note the & - this opens a process not tied to the terminal
- Type some text, save the file, and exit

3.13 which (List where program is installed)

- *which ls*   //List location of ls command
- *which fdisk*   //Lists location of fdisk command
- *which perl*   //Lists location of perl

3.14 w (List current users)

- *w*   //List the users currently logged onto your system

3.15 find (Search file system)

- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *find / -name ssh**   //**Starting at the / directory**, search for files with names that start with ssh
  (Recall * is a wild card. Note all the permission denied messages.)
- *sudo -s*   //Switch to the root user
- *find / -name ssh**   //I typically search as root user to ensure I find all files (no denied messages!)
- *find ssh**   //Searches only the current directory, returns nothing
- *find *.txt*   //Searches for all .txt files in the current directory, returns gedit and nano files

3.16 ps (List processes)

- *ps*   //List minimal information about running processes
- *ps -ef*   //List full information about processes running

3.17 tar (Create archive (like zip))

- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *tar -cvf arch.tar nano.txt gedit.txt* //Put nano and gedit text files into an archive called arch.tar
- Return to the Desktop GUI
- Right click on **arch.tar** and select **Extract Here**
- Note that this extracts nano and gedit to a directory named arch

3.18 grep (Search a file or terminal output)

- *ps -ef | grep gnome*   //Takes the output of ps and pipes it to grep for searching, returning lines
  containing gnome
- Use gedit to create a file named limerick.txt and paste the following text into it:
  There once was a young girl named Ruth
  Who moved to the town of Duluth
  She bought a big house
  But married a louse
  Who slowly dismantled her youth
- Return to the terminal
- *cat limerick.txt | grep Ruth*
- *cat limerick.txt | grep uth*

- *cat limerick.txt | grep u*

3.19 more (Display text a single screen at a time – useful for long files)
- Use gedit to edit limerick.txt.
- Select all text and copy
- Paste the text into the document 10 times.
- Return to the terminal
- *more limerick.txt*

3.20 md5sum (Calculate the md5 hash of a file)
- *md5sum limerick.txt*
- Note: The MD5 checksum of a file serves as a unique identifier for that file. If one bit is changed in a file, its MD5sum changes. The MD5sum of a file is useful for verifying files downloaded correctly.

Please continue to explore Linux commands using online resources, apropos, help and man pages

4. File Permissions
4.1 Introduction
Linux uses Discretionary Access Control (DAC), meaning the owner of a resource dictates rights to the resource. This means the file creator (owner) and root have the ability to control who reads, changes, executes, or deletes the file.

- Open a terminal
- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *ls -al*   //Long listing format including file permissions


```
ace@ace:~/Desktop$ ls -al
total 24
drwxr-xr-x  2 ace  ace  4096 2009-08-28 15:45 .
drwxr-xr-x 30 ace  ace  4096 2009-08-28 15:33 ..
-rwxrw-r--  1 ace  ace     3 2009-08-26 15:55 gedit.txt
-rw-r--r--  1 ace  ace  1832 2009-08-26 16:13 limerick.txt
-rw-r--r--  1 ace  ace    79 2009-08-26 16:01 me.txt
-rw-r--r--  1 root root    5 2009-08-25 13:25 nano.txt
ace@ace:~/Desktop$
```

Permissions, owners, and groups of files stored on the Desktop

Circled in **red** are the file permissions, in **orange** is the file's owner, and in **green** is the file's group. Nine bits of each file are used to store read, write, and execute file permissions.

- **r** = Read permission (e.g. view with gedit)
- **w** = Write permission (e.g. change with nano text editor and save)
- **x** = Execute permission (e.g. execute a perl binary)
- **-** = Unauthorized to read, write, and/or execute

The listing specifies permissions for the file owner, members of the file's group, and all other users. See below a close-up and colorized version of the file permissions for gedit.txt.

- In **black**, the dash specifies gedit.txt is a file. A *d* in this position specifies a directory.
- In **red** are the permissions for the file's owner. The owner may read, write, or execute the file. The owner of gedit.txt is ace.
- In **orange** are the permissions for the file's group. Members of the group may read or write to the file, but may not execute it. The group of gedit.txt is ace.
- In **green** are the permissions for the all other users. All other users may read the file, but may not write to it or execute it.

Note: Set the default file permission for new files in /etc/profile with the umask command. For example, add umask 222 at the end of the profile file to set the default file permission to 555.

4.2 RWX Examples

1) File T permissions are -rwxrwxrwx   Anyone can read, write, or execute T
2) File U permissions are drwxrwxrwx   U is a directory
3) File V permissions are -r--r--r--   Anyone can read V, no one can write to or execute
4) File W permissions are -rwx------   Only the owner can read, write or execute
5) File X permissions are ----------   Root can still read but not write or execute. No one
            else can read, write, or execute.

4.3 Numeric Representation of File Permissions

Computers use bits to store file permissions.
      rwxrwxrwx is stored as 1's and 0s, in this case 111111111

Recall octal (same as decimal from 0-7) / binary equivalents:

Octal	Binary
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

4.4 Numeric Representation Examples

Letter version			Binary version			Octal Version		
Owner	Group	All Other Users	Owner	Group	All Other Users	Owner	Group	All Other Users
rwx	rwx	rwx	111	111	111	7	7	7
rw-	r--	-w-	110	100	010	6	4	2
rwx	--x	rw-	111	001	110	7	1	6
r-x	-wx	---	101	011	000	5	3	0

4.5 chmod (Change RWX File Permissions)

- Open a terminal
- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *ls -al*   //Long listing format including file permissions
- *sudo -s*   //Switch to root
- *chmod 777 limerick.txt*   //Change file permissions so all users can rwx
- *ls -al*
- *chmod 000 limerick.txt*   //Change file permissions
- *gedit limerick.txt*   //Try to read/write file with root privileges

  ◦ Can you read the file with root privileges?

  ◦ Can you edit the file with root privileges?
- *chmod 755 limerick.txt*   //Change file permissions
- *ls -al*

4.6 chown (Change File Owner)

- Open a terminal
- *su ace*   //Ensure ace privileges
- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *touch chown.txt*   //Create file owned by ace
- *ls -al*   //Long listing format including owner
- *sudo -s*   //Escalate to root privileges
- *chmod 770 chown.txt*   //Change file permissions
- *chown root chown.txt*   //Change file owner to root
- *ls -al*   //Long listing format including owner
- *su ace*   //Switch to ace privileges
- *gedit chown.txt*   //Can you read/write chown.txt? Why or why not?

4.7 chgrp (Change File Group)

- Open a terminal
- *cd ~/Desktop*   //Move to the Desktop of the current user ace
- *ls -al*   //Long listing format including group
- *sudo -s*   //Escalate to root privileges
- *chgrp root chown.txt*   //Change file group to root
- *ls -al*   //Long listing format including group
- *su ace*   //Switch to ace privileges
- *gedit chown.txt*   //Can you read/write chown.txt? Why or why not?

5. Review Questions

- Compare and contrast the /bin and /sbin directories

- Assume you have root privileges. Write the terminal commands to change the owner and group of a file named *file.txt* to *galactica* (owner) and *starbuck* (group).

- Write the binary and octal representations of the following file permissions:
  ° -rwxr-x-w-
  ° -rw---xr--

- Compare and contrast the information stored by the /etc/shadow and /etc/passwd files

- Questions a-e refer to the screenshot below:
  ° Who is the owner of superman.txt?
  ° To what group does superman.txt belong?
  ° List the owner privileges for superman.txt
  ° List the group privileges for superman.txt
  ° List all other user privileges for superman.txt

```
root@ace:~/Desktop# ls -al
total 8
drwxr-xr-x  2 ace ace  4096 2009-08-31 11:12 .
drwxr-xr-x 30 ace ace  4096 2009-08-31 10:56 ..
-rwxr----x  1 ace root     0 2009-08-31 11:12 superman.txt
root@ace:~/Desktop#
```

Cyber Fundamentals #3: VMware Snapshots and Ubuntu Package and Account Management

1. Introduction

This brief activity is an introduction to using VMware snapshots and Ubuntu package and account management. You'll make a VMware image snapshot, change the image and revert to the snapshot, install a select set of Ubuntu packages, and create new user accounts.
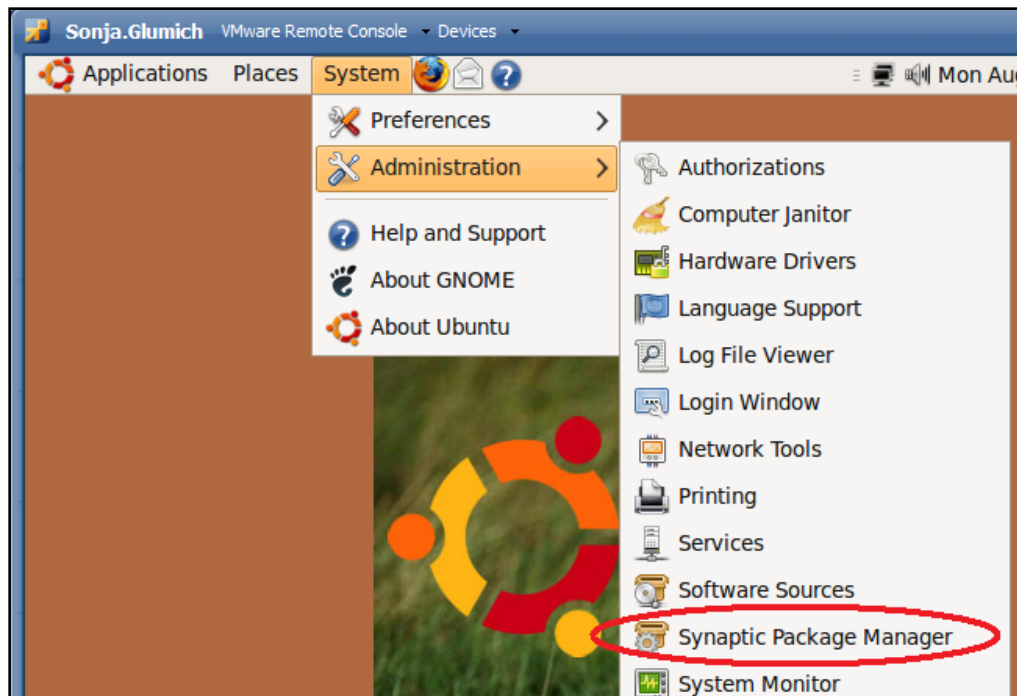
Synaptic for Ubuntu Package Management

1.1 Objectives

- Create an Ubuntu image with VMware

- Take a snapshot and revert to a prior snapshot with VMWare

- Install the **nmap** package with the Synaptic package manager

- Install the **vsftpd** package with the apt package manager

- Update installed packages using the Update Manager

- Create and delete Ubuntu user accounts through the Graphical User Interface (GUI) and the terminal

1.2 Materials

- Windows computer with access to an account with administrative rights

- VMware Server

- Ubuntu OS iso file

1.3 Assumptions

- The provided instructions were tested on a Windows Vista physical machine. Instructions may vary for other OS

- The student has administrative access to their system and possesses the right to install programs

- The student's computer has Internet access

1.4 Random Notes

- A *Jackalope* is a mythological animal that is a cross between a jackrabbit and an antelope

- *Ubuntu,* an African word, means *Humanity to others*

2. VMware Snapshots

2.1 What is a Snapshot?

Snapshots capture an image in an instance of time and can serve as a "known good state" for system backup and restore. Imagine you have a website. You install the website on a VMServer image, take a snapshot, and make the website available to the public. Someone hacks your image and deletes all of your website files. If the compromise is limited to the image (doesn't include the host), you can revert to the initial snapshot, (hopefully) mitigate the vulnerability the attacker exploited, take an updated snapshot, and put the site back online. (Note: In this case it would be smart to make additional offline copies of the website files and the VMware image.)

2.2 Create a Snapshot

- Power on and log into the Ubuntu image

- From the VMware Web Access page, select ***Virtual Machine > Take Snapshot***
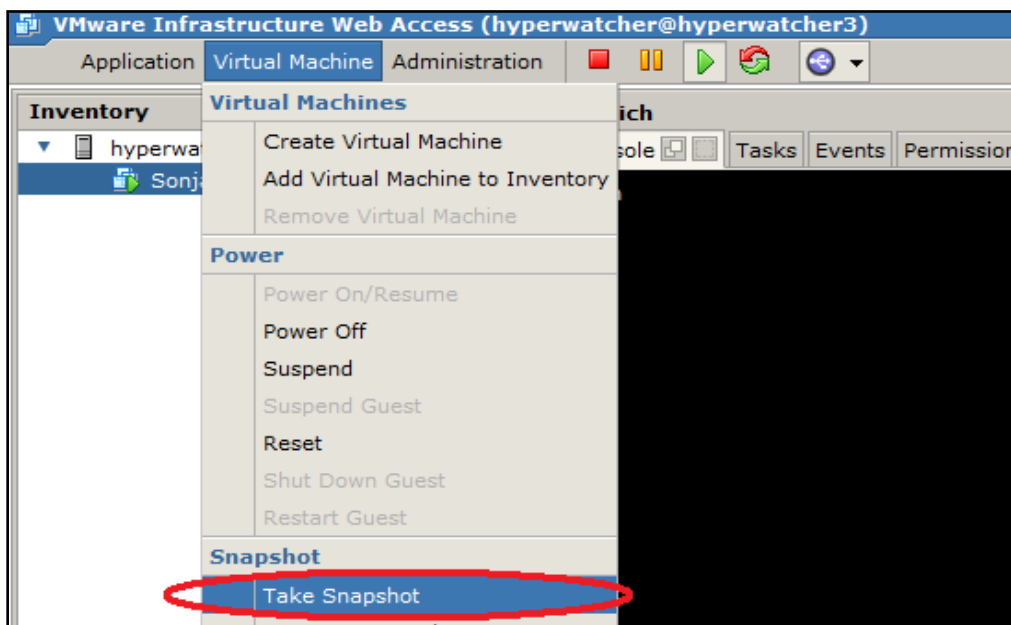
- Return to the image, right click on the Desktop, select ***Change Desktop Background,*** choose a different background image, and click on ***Close***. Make any other changes (open a terminal or other programs, etc.) you wish.

2.3 Revert to the Prior Snapshot

- Return to the VMware Web Access page and select *Virtual Machine > Revert to Snapshot*
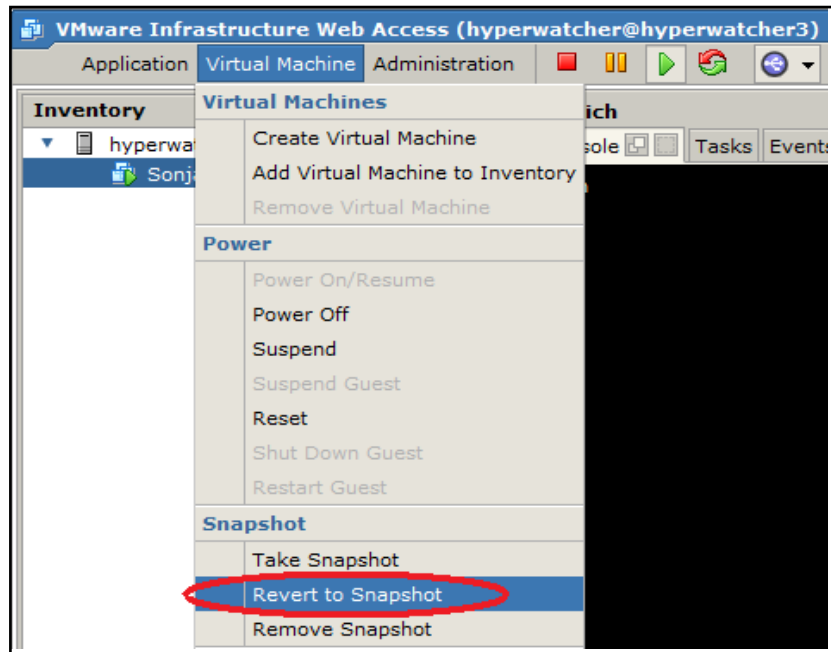
- Return to the image. The Desktop image and anything else you changed will have reverted to state at the time of the snapshot

- VMServer can only save a single snapshot. Taking a second snapshot will overwrite the first. VMWorkstation (costs $) can save multiple snapshots.

3. Ubuntu Package Managers

3.1 What is a Package?
In the past, users downloaded Linux software as source, configured it, compiled it, and installed it. This process was tedious and error prone. Today, most Linux software is available in packages, software pre-built for a specific OS version. Packages combined with package managers such as **Synaptic** and **apt** makes installing software packages on Linux often easier than installing software on Windows.

3.2 The Synaptic Package Manager
- Synaptic Package Manager is a GUI used to easily install/uninstall/update software

- To start Synaptic select *System > Administration > Synaptic Package Manager*
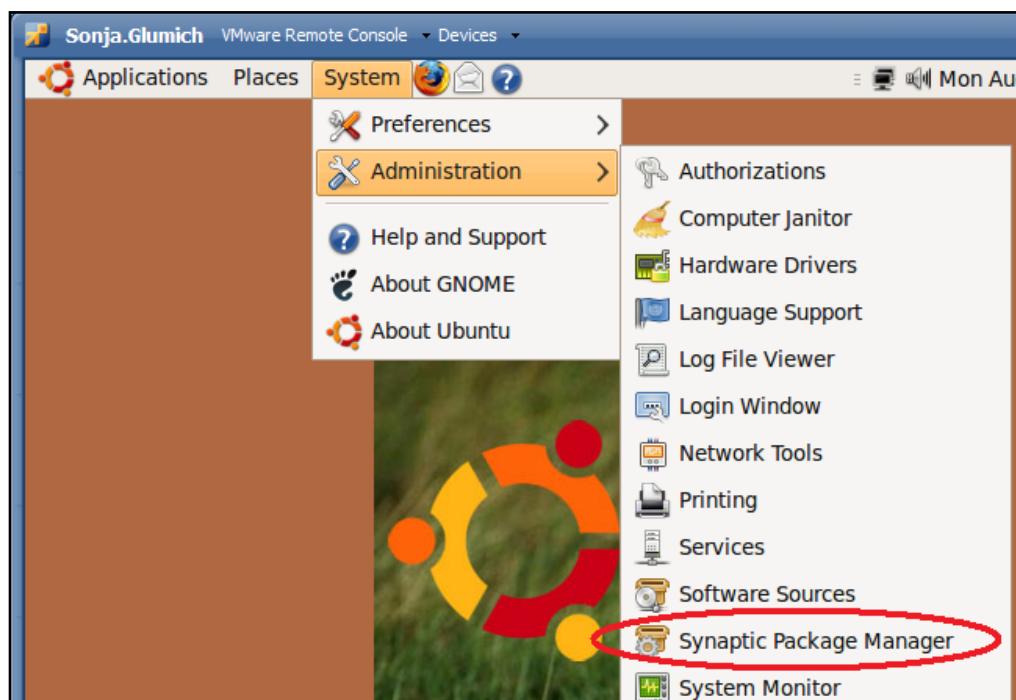
- Synaptic will start, listing packages available for download from remote repositories (you must have an Internet connection to install from remote repositories)

- Synaptic enables browsing for packages by category, searching for a packages by name or keyword, and updating currently installed packages to the latest version

- To install a package, simply select the *box* preceding the package name, click *Mark for Installation*, and click *Apply*

- See below for a search for *netcat*, which is already installed
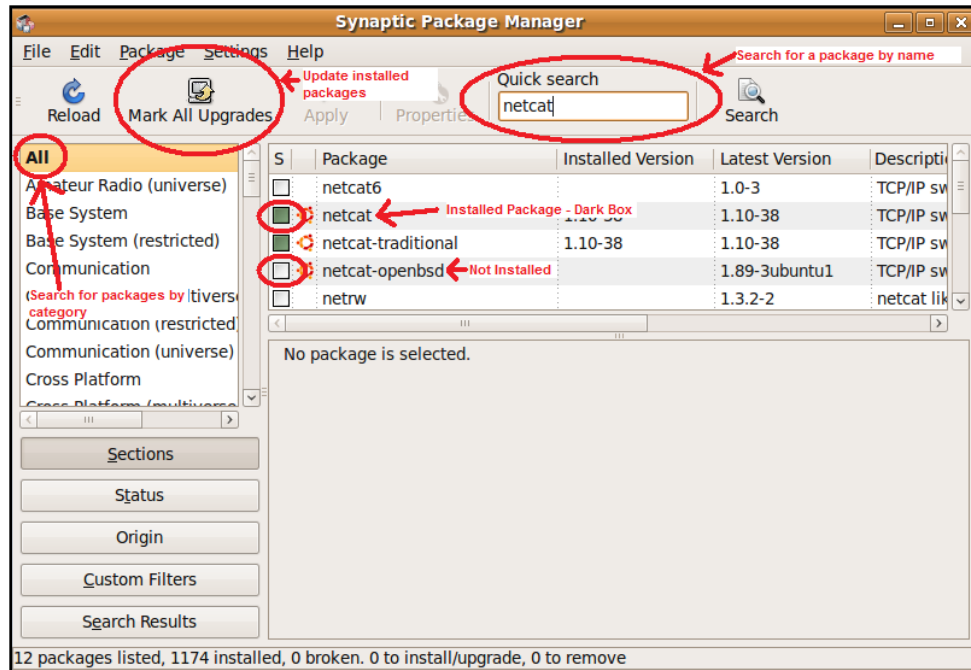
- Use Synaptic to install the ***nmap*** package

3.3 The apt Package Manager

To optimize system performance, Linux servers often have no GUI installed and require the terminal for user input. The apt-get command-line utility provides functionality similar to Synaptic.

- Open a terminal
- ***sudo -s***   (to get root privileges)
- ***apt-get update***   //Ensures most up-to-date listing of packages
- ***apt-get upgrade***   //Upgrades outdated packages to the current version
- ***apt-get install <package name>***
    - Install new package
    - Ex. ***apt-get install nmap***
- ***apt-cache search <package name>***
    - search for packages
    - Ex. ***apt-cache nmap***
- ***apt-cache dump***
    - Lists all packages
    - Try ***dpkg -l*** for a more concise listing
- ***apt-get upgrade***   //Upgrade all outdated packages
- ***apt-get install vsftpd***   //Install the ***vsftpd*** package

4. Create Ubuntu User Accounts

As with most things in Ubuntu, there are multiple ways to create accounts. Two of the ways are through the User Settings GUI and the *adduser* command.

4.1 The Users and Groups GUI

- Select *System* > *Administration* > *Users and Groups*

- Select *Unlock* and enter your password

- Select *Add User*
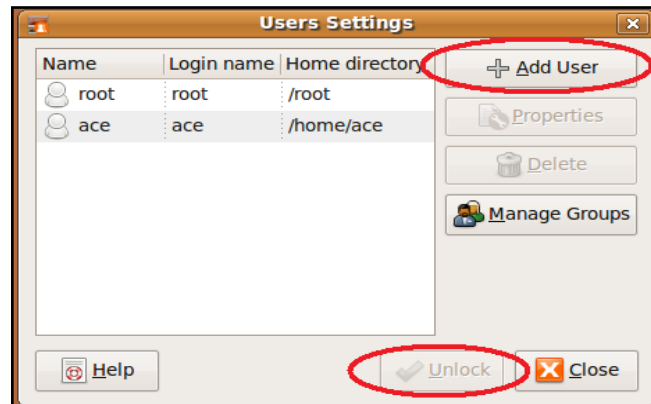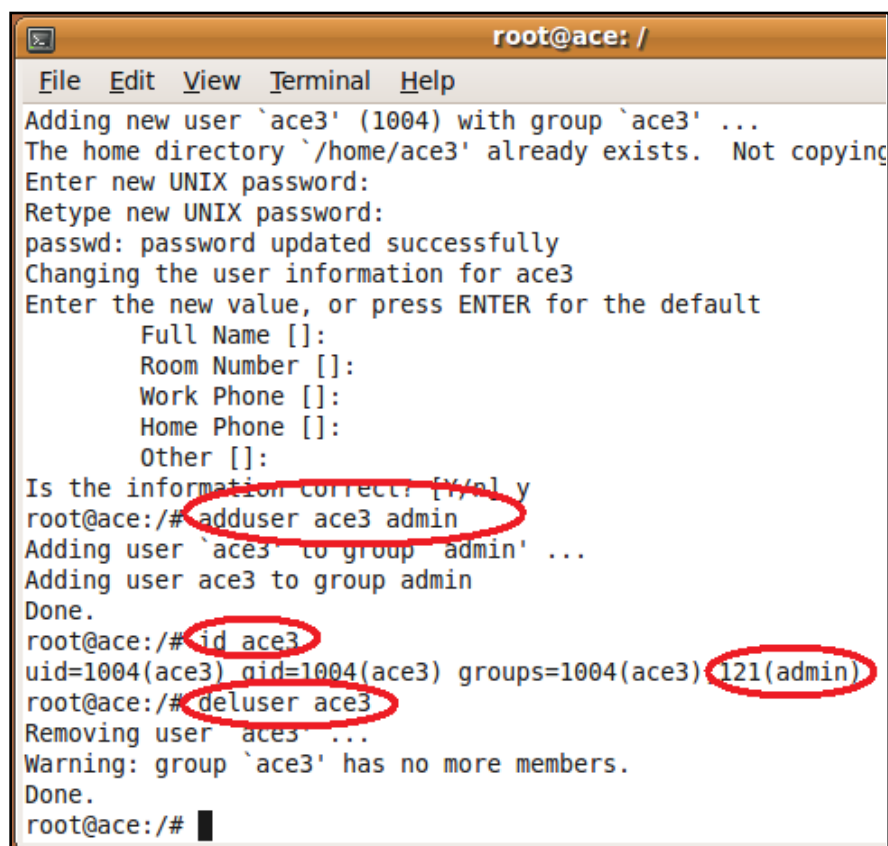
- Create account *ace2* with password *ilikeace*

- Select the different profiles (Administrator, Unprivileged, Desktop User) and click on the *User Privileges* tab to view the privileges associated with each profile

- Note that while the Administrator has almost all privileges by default, Unprivileged has no default privileges. Make ace2 a *Desktop user* which imparts moderate privileges.
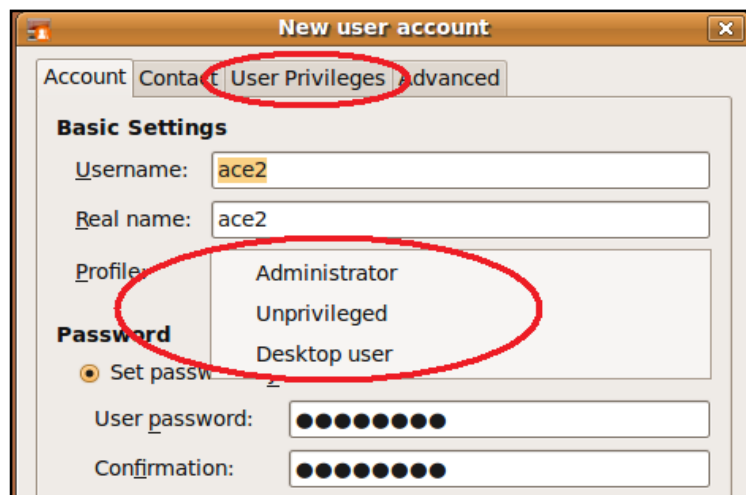
4.2 The Command Line (adduser)

- Open a terminal

- Type sudo -s and enter your password to gain root privileges

- **Create Account:**
  - Type adduser ace3 and follow the prompts
  - This creates an account with very limited privileges (unprivileged account)
  - Type id ace3 – note the ace3 account isn't assigned to any groups

- **Add User to a Group:**
  - Upon joining a group, a user will inherit any privileges assigned to the group
  - Type adduser ace3 admin to add ace3 to the administrators group
  - Type id ace3 – note the ace3 account is now assigned to the admin group

- **Delete Account:**
  - Type deluser ace3 to delete the ace3 account

```
root@ace: /

File   Edit   View   Terminal   Help

Adding new user `ace3' (1004) with group `ace3' ...
The home directory `/home/ace3' already exists.  Not copying
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for ace3
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@ace:/# adduser ace3 admin
Adding user `ace3' to group `admin' ...
Adding user ace3 to group admin
Done.
root@ace:/# id ace3
uid=1004(ace3) gid=1004(ace3) groups=1004(ace3) 121(admin)
root@ace:/# deluser ace3
Removing user `ace3' ...
Warning: group `ace3' has no more members.
Done.
root@ace:/#
```

5. Review Questions
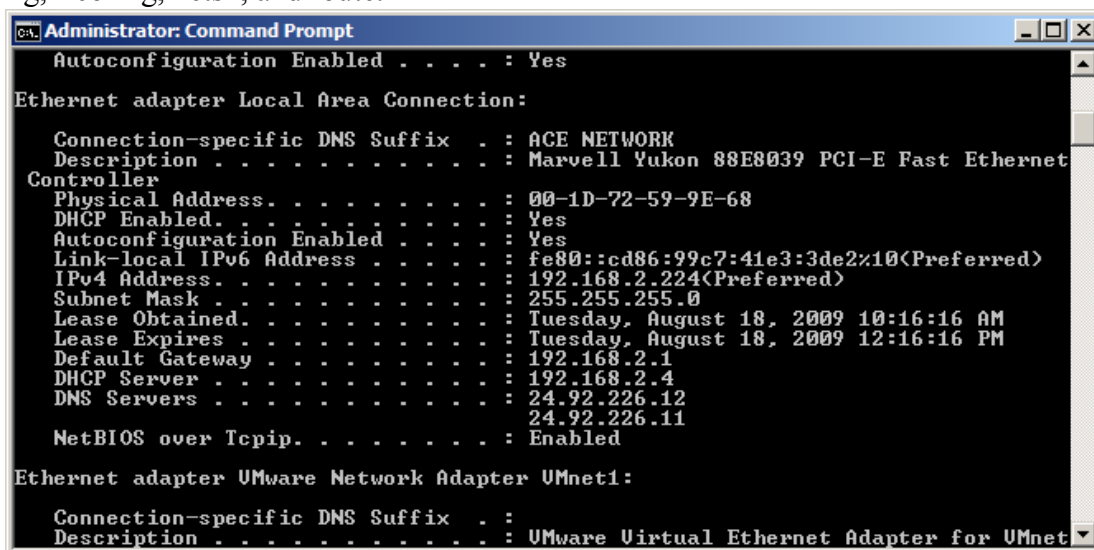
- Write an Ubuntu Linux command to determine the group ID for a user named clark.

- Write a single Ubuntu Linux terminal command to search for a package named wallyworld.

- What is one difference between VMServer and VMWorkstation?

- Write an Ubuntu Linux command to add a new user named ellen

- Write an Ubuntu Linux command to add user ellen to a group named rusty.

Cyber Fundamentals #4: Windows and Linux Network Configuration

1. Introduction

Establishing network connectivity in Windows and Linux follows a similar process. Steps include setting the computer's Internet Protocol (IP) address, the addresses of the Domain Name Servers (DNS) servers, and the route to the gateway (the gateway links an internal network to external networks).

This review examines the processes and resources involved in managing network configuration on Windows and Linux machines. It includes an overview of useful networking commands like ipconfig, ifconfig, netsh, and route.

Windows Vista Command Prompt – ipconfig Command Output

1.1 Objectives

- Review basic network concepts

- Configure Windows and Linux to connect to a network

- Review the ping, netstat, ipconfig/ifconfig, and route commands

1.2 Materials

- Windows computer with access to an account with administrative rights

- VMware Server

- Ubuntu OS iso file

1.3 Assumptions

- The provided instructions were tested on a Windows Vista physical machine and an Ubuntu Jaunty Jackalope VMware virtual machine. Instructions may vary for other OS.

- The student has administrative access to their system and possesses the right to install programs

- The student's computer has Internet access

1.4 Random Notes

- Like Linux, Macintosh (based on Unix) provides the ifconfig command

- ifconfig stands for "interface configurator"

- ipconfig stands for "internet protocol configuration"

2. Basic Networking Concepts

2.1 What is a Network Packet?
A packet is discrete amount of data (think a finite string of 1s and 0s) structured in a particular format.

001011101

If (first 3 bits == 001) {Evacuate}
If (middle 3 bits == 011) {Fire}
If (last 3 bits == 010) {Rome, NY Office}

If (first 3 bits == 111) {Stay Indoors}
If (middle 3 bits == 000) {Poison Gas Attack}
If (last 3 bits = 101) {Chicago, IL Office}
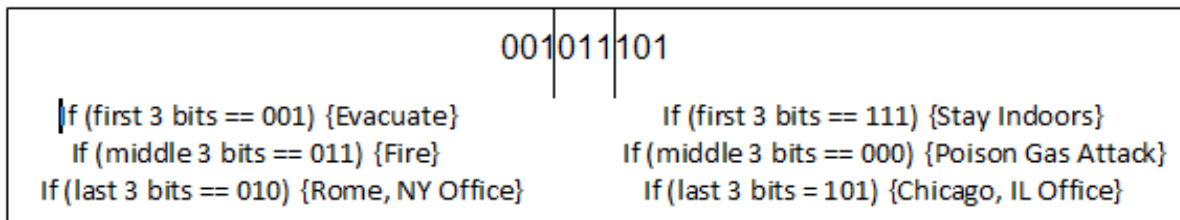
The order of 1s and 0s in a packet impart additional meaning

A computer sending data over a network divides the data to be transmitted into packets and sends them to the remote system, which reassembles the packets into the original data.

Data   Packets

192.168.1.9

Internet

Packets   Data

66.123.4.22
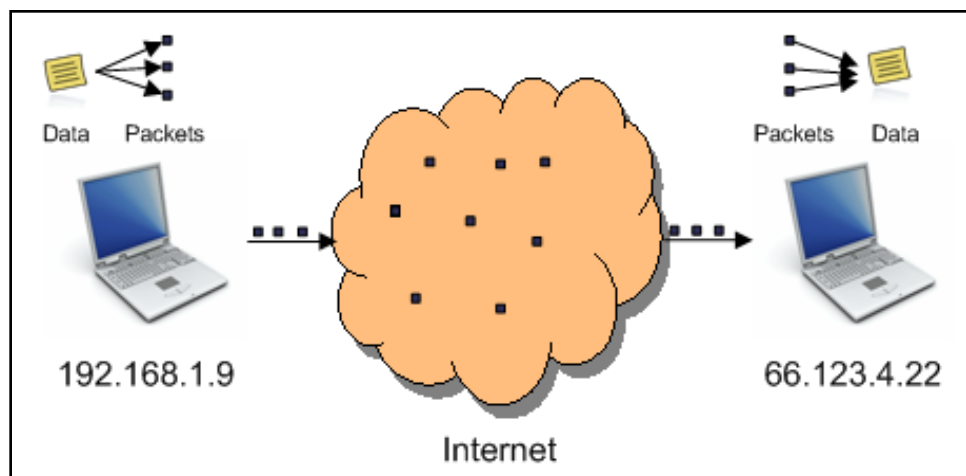
Data disassembled into packets, routed independently through a network, then reassembled

2.2 What is an IP Address?

An IP Address uniquely* identifies computers on a network, enabling computers to send and receive packets. Computers mark packets with the source (sender) and destination (recipient) IP addresses. IP addresses take the format W.X.Y.Z, where W, X, Y, and Z range between 0 and 255 (decimal).

Comparing a packet to a letter, the sending or source (src) computer's IP address is similar to the return address of the sender of a letter. The IP address of the receiving or destination (dst) computer is similar to the street address of the building receiving the letter.

In some cases computers use duplicate IP addresses...but this discussion is too in-depth for this brief review

2.3 What is a Port Number?

Computers often also mark packets with the source (sender) and destination (recipient) port numbers. If an IP address is similar to a street address of a building, the port number is like an apartment number. The port number tells the receiving computer which of its many running applications (which of many apartments in a building) should receive the packet. For example, Firefox and an FTP client might send information to the same IP address (same computer) but different port numbers (different applications running on the same computer).
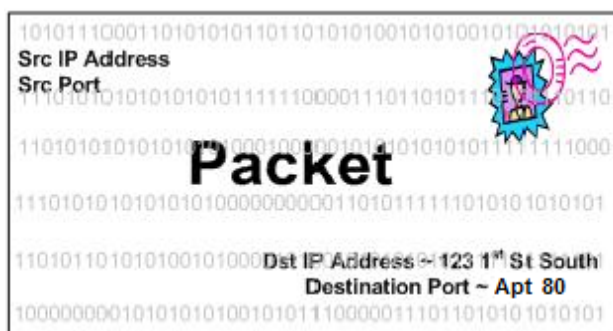
Packet addressed to a Web Server at 123 1ˢᵗ St S
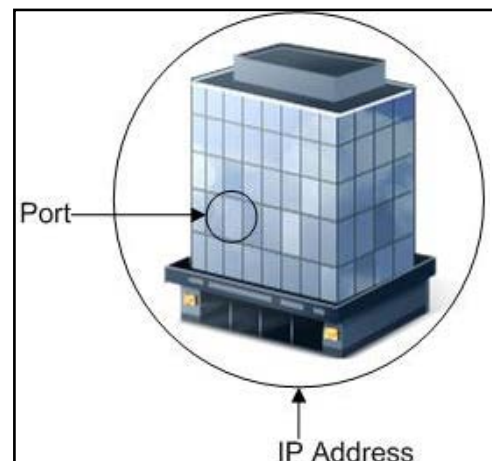
The Apache Web Server lives in Apt 80 (Port)
The Filezilla FTP Server lives in Apt 21 (Port)
Both live at the same Street Address (IP Address)

2.4 What is Dynamic Host Configuration Protocol (DHCP)?
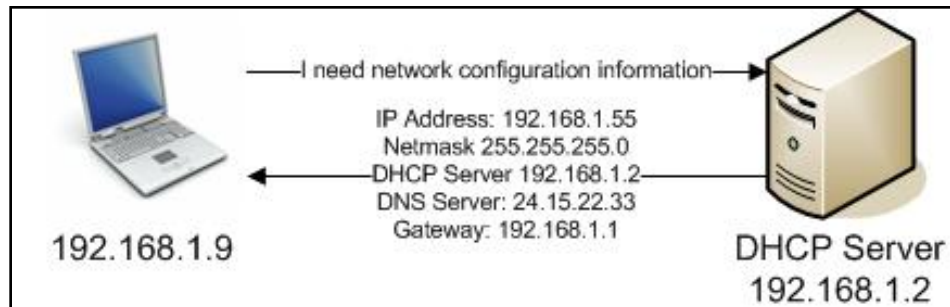
Dynamic Host Configuration Protocol is a network protocol used by clients (like your own computer) to retrieve network configuration information from a server. This information allows the client to communicate on the network.

2.5 What is Domain Name System (DNS)?
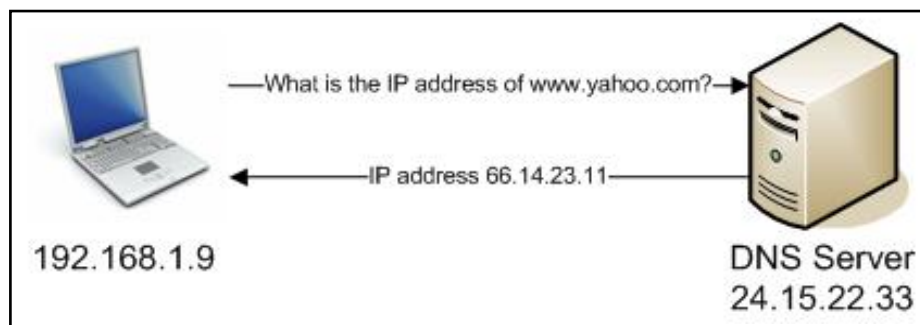
Q: Would you enjoy typing IP addresses (like 64.233.169.147) **in your web browser every time you wanted to visit a web page (like the Google home page)?**

A: Probably not. Humans remember names or phrases far better than seemingly meaningless strings of numbers. However computers such as routers work with IP addresses, not domain names. Luckily, Domain Name System (DNS) servers translate domain names humans type into browsers (www.google.com) into IP addresses (64.233.168.147). Bottom line: if your computer can't reach a DNS server, you won't be able to browse the Internet using domain names (no www.netflix.com for you!).

Q: How does a computer locate a DNS server?

A: There are many publicly available DNS servers. A computer may obtain the IP address of a DNS server from a DHCP server or a user can specify the DNS server IP address manually through a GUI or in a configuration file.

3. Internet Protocol (IP) Addresses

A user manually sets a **static IP address**. It does not typically change over time*. A DHCP server automatically sets a **dynamic IP address**. The DHCP server leases a computer an IP address for a certain amount of time. When the lease expires, the system may receive a different address from the DHCP server (although it tends to remain the same).

***Unless the user manually changes the address or enables dynamic addressing.

3.1 Setting a Static IP Address - Windows Terminal
- Open a Windows terminal

- Type *netsh interface ip show config* to see network configuration information

- Type *ipconfig /all* for another method of viewing network configuration information

- Look at the entry for *"Local Area Connection"*** and note the IP address, Subnet Mask (netmask), default gateway, DHCP server, and DNS servers

- Type *netsh interface ip set address name="Local Area Connection" static 192.168.1.100 255.255.255.0 192.168.1.1 1* to manually set the following:
  - Static IP address to 192.168.1.100
  - Netmask to 255.255.255.0
  - Gateway to 192.168.1.1
  - Gateway Metric to 1 (don't worry about this field)

**It may also be something like *Local Area Connection 3*. If using a wireless connection, insert *"Wireless Network Connection"* everywhere you see *"Local Area Connection"*

3.2 Setting a Dynamic IP Address (DHCP) - Windows Terminal
- Type *netsh interface ip set address "Local Area Connection" dhcp* to dynamically fetch IP address and other configuration information from a DHCP server.

- Type *ping www.yahoo.com* to verify connectivity. If you have connectivity issues and get stuck, use *ipconfig /all* to verify the network configuration information is correct and/or restart the system.

3.3 Setting Static and Dynamic IP Addresses - Windows GUI

- Go to *Start* > *Control Panel* > *Switch to Classic View* > *Network Connections*

- Right click *Local Area Connection* (or Wireless Network Connection if using Wireless)

- Select *Properties*

- Select *Internet Protocol Version 4 (TCP/IPv4)* and click on *Properties*
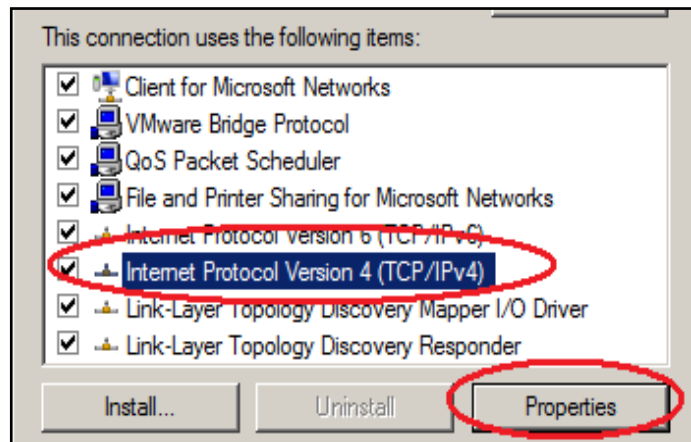
- For steps 7 and 8, leave your network settings the way they are (**or first take a screenshot to ensure you can revert them back to the way you found them**)

- To set the IP address and DNS servers dynamically using the DHCP server, you'd select the options highlighted below:
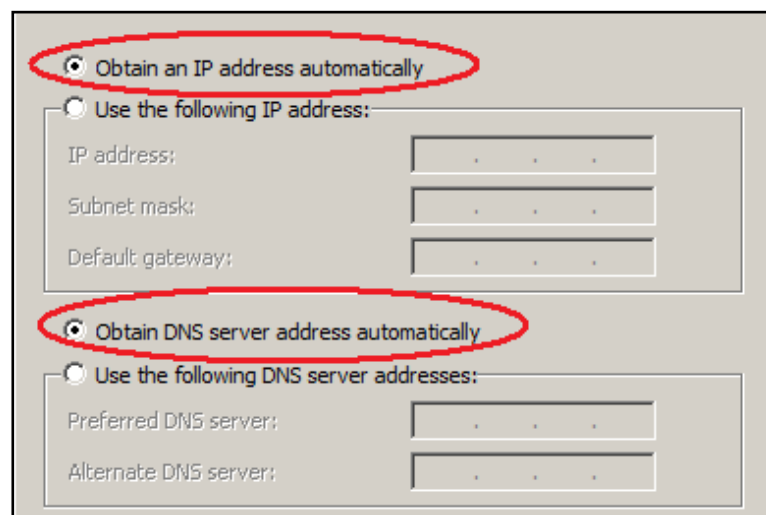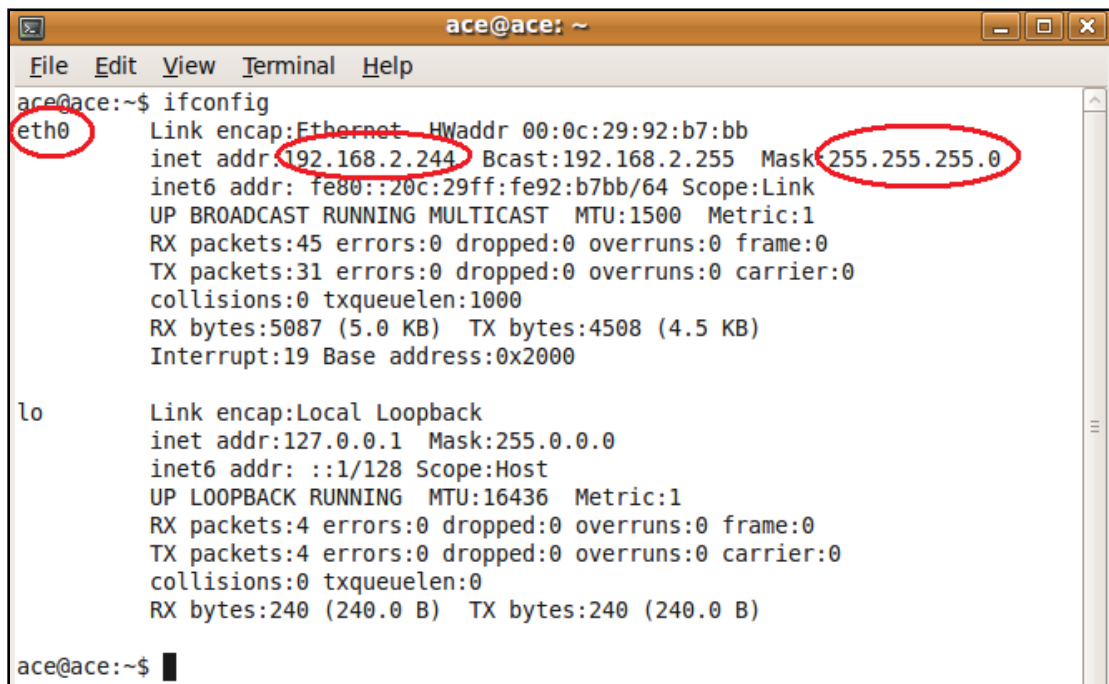
- To set a static IP address and DNS servers manually, you'd select the options highlighted below and manually fill in the information as shown:

3.4 Setting a Temporary Static IP Address in Linux

- In Ubuntu, open a terminal and sudo to root (*sudo -s*)

- Type *ifconfig* to view network configuration information. Note that your system may use a different interface than eth0 (wlan0, eth1, eth2...).

```
                                      ace@ace: ~

File   Edit   View   Terminal   Help

ace@ace:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:92:b7:bb
          inet addr:192.168.2.244  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe92:b7bb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5087 (5.0 KB)  TX bytes:4508 (4.5 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:240 (240.0 B)  TX bytes:240 (240.0 B)

ace@ace:~$
```
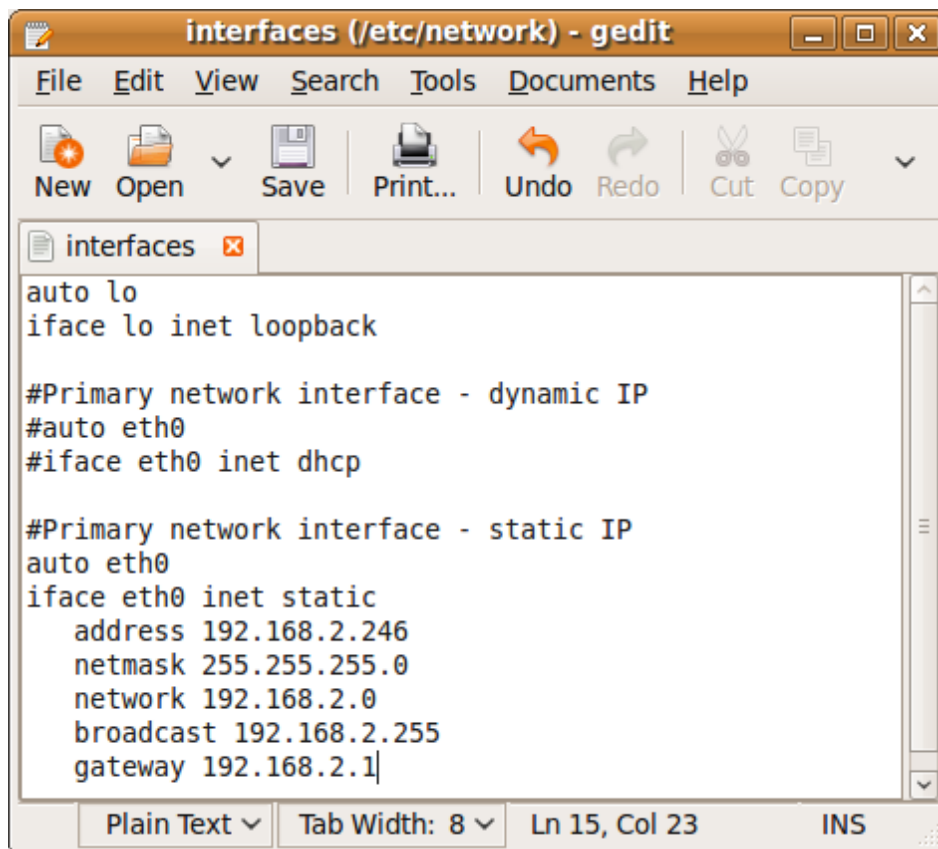
- Record the original IP address and netmask

- Type *ifconfig eth0 192.168.1.100 netmask 255.255.255.0*

- Type *ifconfig eth0* to verify the change

- If you restarted your system at this point, your ifconfig changes would be lost

- Type *ifconfig eth0 <original IP address> netmask <original netmask>*

- Type *ifconfig eth0* to verify the change

- Type *ping www.yahoo.com* to verify connectivity. If you have connectivity issues, try requesting an IP address from your DHCP server (*dhclient*) or restarting the image.

3.5 Setting a Persistent Static IP Address in Linux

- Open a terminal and sudo to root to enable running gedit with root privileges (*sudo -s*)

- Use gedit to open /etc/network/interfaces (*gedit /etc/network/interfaces*)

- If you see the below lines, comment them out (precede comments by the **#** sign)
      #auto eth0
      #iface eth0 inet dhcp

- Assuming eth0 is your primary interface add the following to the *interfaces* file:
      #The primary network interface – static IP
      auto eth0
      iface eth0 inet static
            address 192.168.1.100
            netmask 255.255.255.0
            network 192.168.1.0
            broadcast 192.168.1.255
            gateway 192.168.1.1

Setting a persistent static IP address in Linux

- From the command line, run *ifconfig eth0* and note the address is unchanged

- Type */etc/init.d/networking restart* to reload network configuration parameters

- Type *ifconfig eth0* again and note the address has now changed

- Type *shutdown -r now* to restart the image

- Log back in and rerun *ifconfig eth0* – note the address is still set to the static value

3.6 Setting a Dynamic IP Address in Linux

1. Open a terminal and sudo to root to enable running gedit with root privileges (*sudo -s*)

2. Use gedit to open /etc/network/interfaces (*gedit /etc/network/interfaces*)

3. Assuming eth0 is your primary interface, comment out the static IP lines and uncomment the dhcp lines. The interfaces file should now look like:

```
auto lo
iface lo inet loopback

#Primary network interface - dynamic IP
auto eth0
iface eth0 inet dhcp

#Primary network interface - static IP
#auto eth0
#iface eth0 inet static
#    address 192.168.1.246
#    netmask 255.255.255.0
#    network 192.168.1.0
#    broadcast 192.168.1.255
#    gateway 192.168.1.1
```

Setting a dynamic IP address in Linux

4. From the command line, run *ifconfig eth0* and note the IP address is unchanged

5. Type */etc/init.d/networking restart* to reload network configuration parameters. Note how the Ubuntu system requests an IP address from the DHCP server.

6. Type *ifconfig eth0* again and note the address has now most likely changed (although it is possible the DHCP server would give you the same address as the static IP you set)

7. If you have connectivity issues, type *dhclient* to request an IP address from the DHCP server.

4. Routes and the Default Gateway

4.1 What is a route?
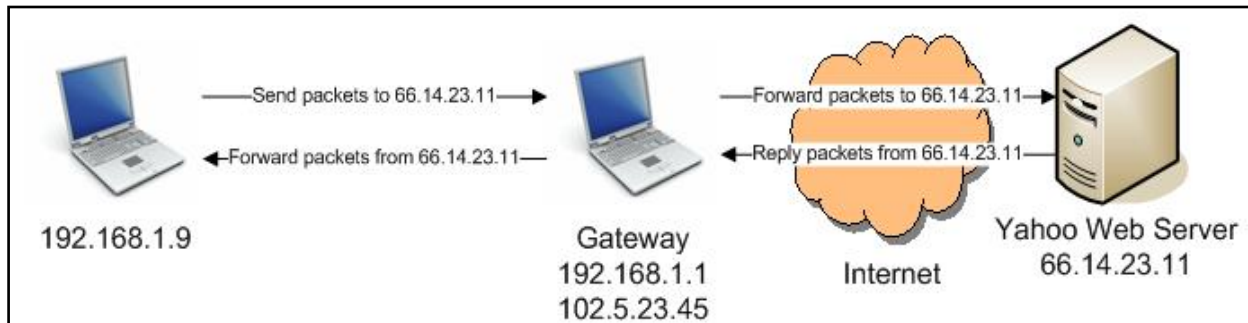
Packets Travel through a Gateway to Reach Internet Resources Outside the LAN

The word *route* refers to the path a packet takes as it travels from a source to a destination. There are typically many paths a packet can travel. The route indicates which path a packet should take. The route is stored in the ***Kernel IP Routing Table.***

4.2 What is the Default Gateway?

Think of the ***default gateway*** as the gatekeeper between your local area network and the rest of the Internet. To reach anything outside the Local Area Network (LAN) on the rest of the Internet, packets must travel through the gateway. So if you want to visit www.yahoo.com, your computer has to know the IP address of the gateway, which will forward the packets along the path to www.yahoo.com.

4.3 Setting the Default Gateway in Windows

See sections 3.1 (terminal) and 3.3 (GUI) for a refresher in setting the Gateway in Windows.

4.4 Viewing the Route in Linux

1. Open a terminal and sudo to root (***sudo -s***)

2. Type ***route*** to view the current route

3. Alternately, type ***netstat -rn*** to view the kernel routing table

4.5 Setting the Default Gateway in Linux

4.5.1 Persistent when using a Static IP
See section 3.5 for a refresher in setting the default gateway in the ***interfaces*** file.

4.5.2 Transient with the Route Command
- Use the ***route add*** command to set a transient static route (won't last through a reboot)

- Example: ***route add default gw 192.168.1.1*** to set the route to a gateway at 192.168.1.1

4.6 Deleting the Route in Linux – Transient
m) Type ***route del <destination>*** to delete a route
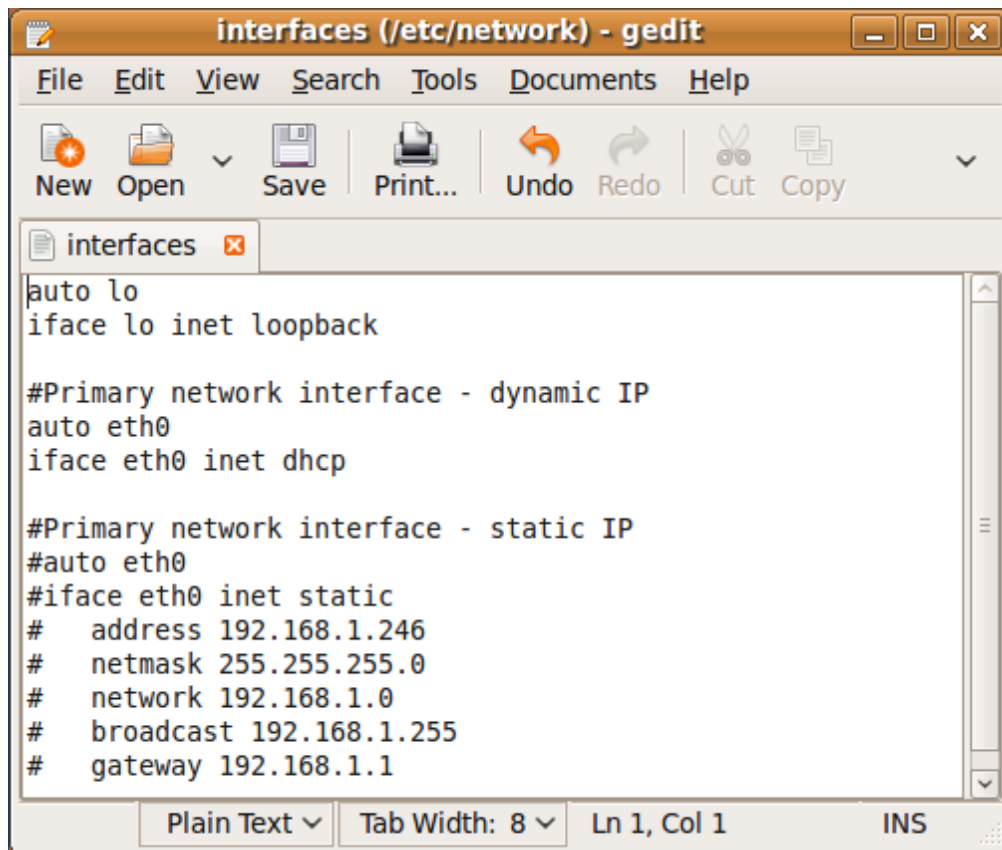
n) Example: ***route del default***

o) If the route is set by a DHCP server or statically in interfaces, this change won't persist through a reboot (the route will reappear)

5. Review Questions

- Write the terminal command to temporarily change the IP address of an Ubuntu box to 192.68.1.5 with a netmask of 255.255.255.0.

- Write the terminal command to temporarily change the default gateway route of an Ubuntu box to 192.168.1.1.

- Which file in Ubuntu stores static network configuration information (such as IP address, netmask, gateway, etc.)?

- Explain how to change from static to dynamic addressing:
  - On Windows
  - On Ubuntu

- Explain the screenshot below:


```
auto lo
iface lo inet loopback

#Primary network interface - dynamic IP
auto eth0
iface eth0 inet dhcp

#Primary network interface - static IP
#auto eth0
#iface eth0 inet static
#    address 192.168.1.246
#    netmask 255.255.255.0
#    network 192.168.1.0
#    broadcast 192.168.1.255
#    gateway 192.168.1.1
```
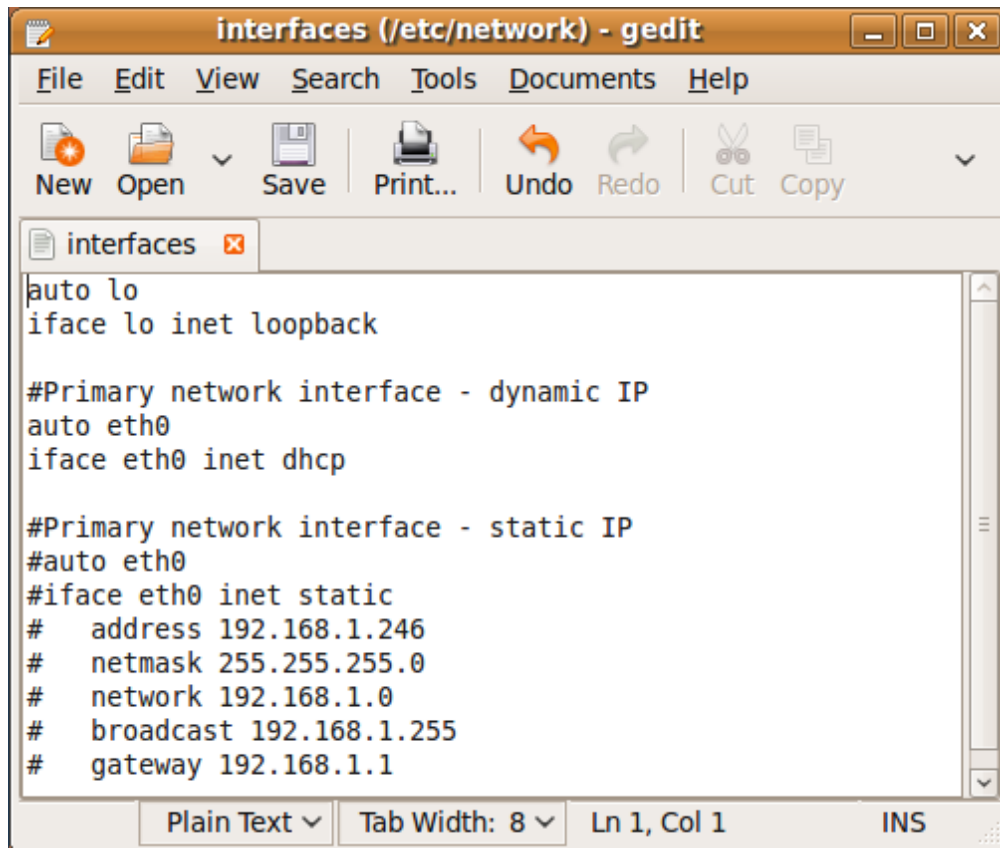
Cyber Fundamentals #5: Wireshark

1. Introduction

Wireshark is a free, open source network traffic analyzer. From a security perspective Wireshark is both a blessing and a bane. Security professionals use Wireshark to view and filter network traffic and analyze network events. Attackers use Wireshark (and its wireless cousins like Kismet) to view and filter packets sniffed by pcap containing passwords and other information from unsuspecting victims.

Every TCP/IP layer adds its own data to a packet. The Application layer adds data. The Transport layer adds a Transport header. The Internet and Network interface layers add their own headers. This exercise involves installing Wireshark and using it to view, filter, and analyze packet header data at each layer of the TCP/IP model.
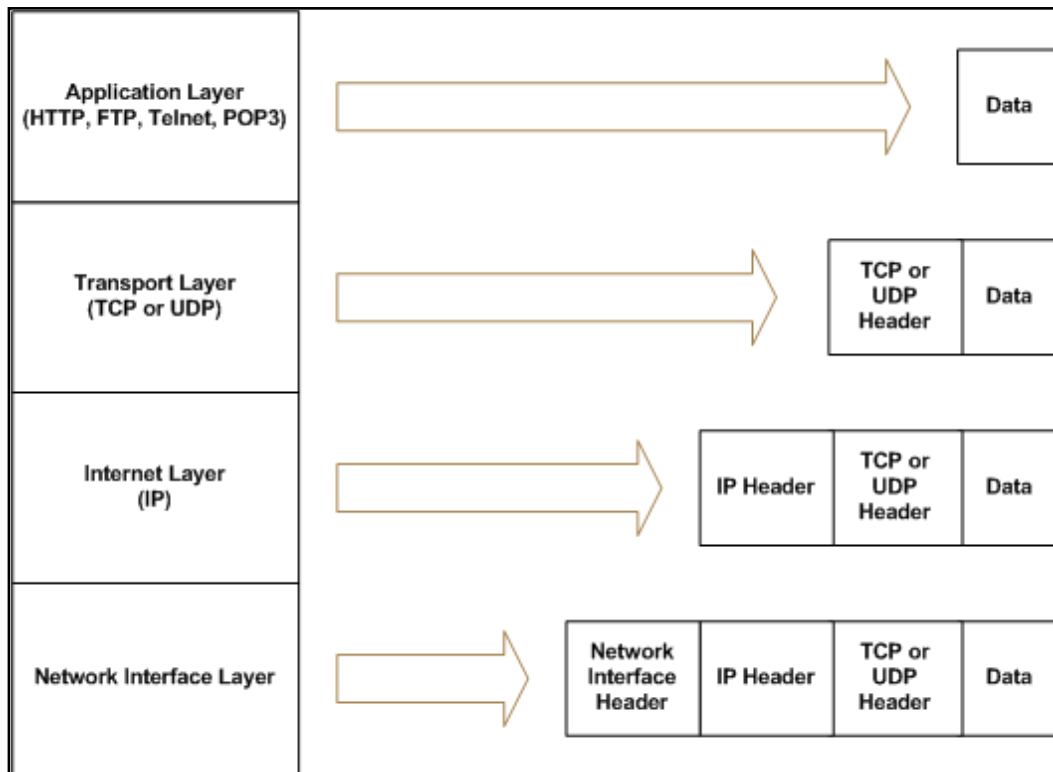
Each layer adds its own data to packets

1.1 Objectives

- Install WinPCap and Wireshark

- Explore the Wireshark Graphical User Interface (GUI)

- Sniff, filter, and analyze network traffic with Wireshark

- Define the four layers of the TCP/IP reference model

- List the protocols at each layer of the TCP/IP model

- Examine packet header data with Wireshark

- Define the header fields of Ethernet frame, Internet Protocol (IP), Transport Control Protocol (TCP), and User Datagram Protocol (UDP) packets

- Draw different types of packet headers, including the header fields and their values.

- Compare and contrast IP, TCP, and UDP

1.2 Materials

- Computer with access to an account with administrative rights

- VMware Server

- Ubuntu OS iso file

- Wireshark and WinPcap

1.3 Assumptions

- The provided instructions were tested on a Ubuntu Jaunty Jackalope image running on a Windows Vista physical machine. Instructions may vary for other OS.

- The student has administrative access to their system and possesses the right to install programs

- The student's computer has Internet access

2. Start Sniffing: Perform a Live Capture of Network Traffic

- From the Wireshark GUI, select *Help > Contents*.

- Peruse the help screens and explore the different menu options to get a feel for the GUI.

- Select *Help > Wireshark Online > User's Guide.*

- Explore the online user's guide.

- Exit the user's guide and return to the Wireshark GUI.

- Select *Capture > Interfaces*.

- Select the *Capture* button on the interface you wish to capture traffic on.

- Select the *Stop* button.

- Select *Capture > Options*.

- Under *Display Options*, select *Update list of packets in real time* and *Automatic scrolling in live capture* to begin a Live Capture.

- Select *Start*, then *Continue without Saving*.

- After a minute or two, stop the capture.

3. Explore the Wireshark GUI: Four Areas of Interest

3.1 Filter Packets with the Filter Bar

- The filter bar enables filtering packets by protocol, IP address, port, flags, sequence number, and many other packet attributes.

- Type *ip* into the filter textbox and click *Apply*. This shows only the Internet Protocol packets. (Note that tcp, http, and other packets are also classified as Internet Protocol.)

- Type *tcp* into the filter textbox and click *Apply.* This shows only the Transport Control Protocol packets. (Note that http and possibly other types of packets are classified as TCP packets.)

- Type *udp* into the filter textbox and click *Apply.* This shows only the User Datagram Protocol Packets. (Note that NBNS and possibly other types of packets are classified as UDP packets.)

- Type *http* into the filter textbox and click *Apply.* This shows only the HyperText Transport Protocol Packets.

- Type *ip.addr==your IP address* and click *Apply* to filter out all but your computer's traffic. (Ex. if your ip address is 10.10.10.2 type *ip.addr==10.10.10.2* and click *Apply*.)

- Select *Clear*
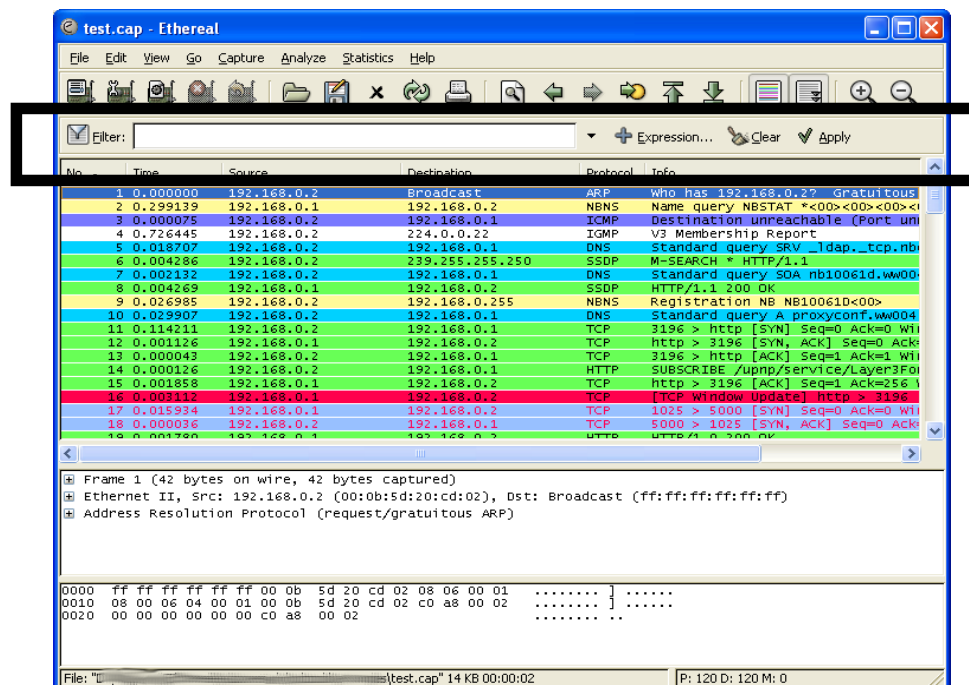
Wireshark filter bar

3.2 View Packet Summaries with the Packet List Window

- **Packet number (No.)**: Numbers each packet starting with 1 for the first packet

- **Timestamp (Time)**: Default is the number of seconds since the beginning of capture

- **IP Addresses (Source, Destination)**: The source and destination addresses of the packet

- **Protocols (Protocol)**: The packet protocol (TCP, UDP, NBNS, etc.)

- **Additional Protocol Information (Info)**: (Example, for a TCP packet, this field states if it is a SYN, ACK, or FIN packet.)

Wireshark Packet List Window

3.3 Study Packet Details with the Packet Details Window

- If you highlight a packet in the *Packet List Window*, further information about the packet appears in the *Packet Details Window*

- Select a packet in the *Packet List Window* and view the information in the *Packet Details Window*.

- Select packets with different protocols. Do the types of information in the *Packet Details Window* change?
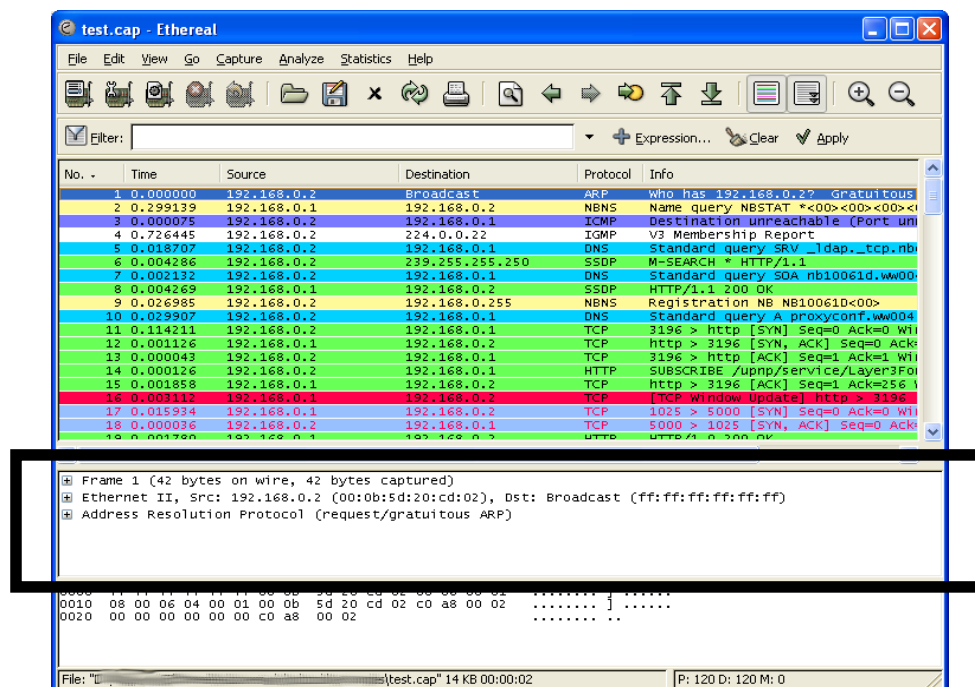
Wireshark Packet Details Window

3.4 View Packet Data with the Individual Packet Bytes Window

- The *Packet Bytes Window* shows the packet data in hexadecimal and ASCII text form

- Select different packets and study the *Packet Bytes Window*
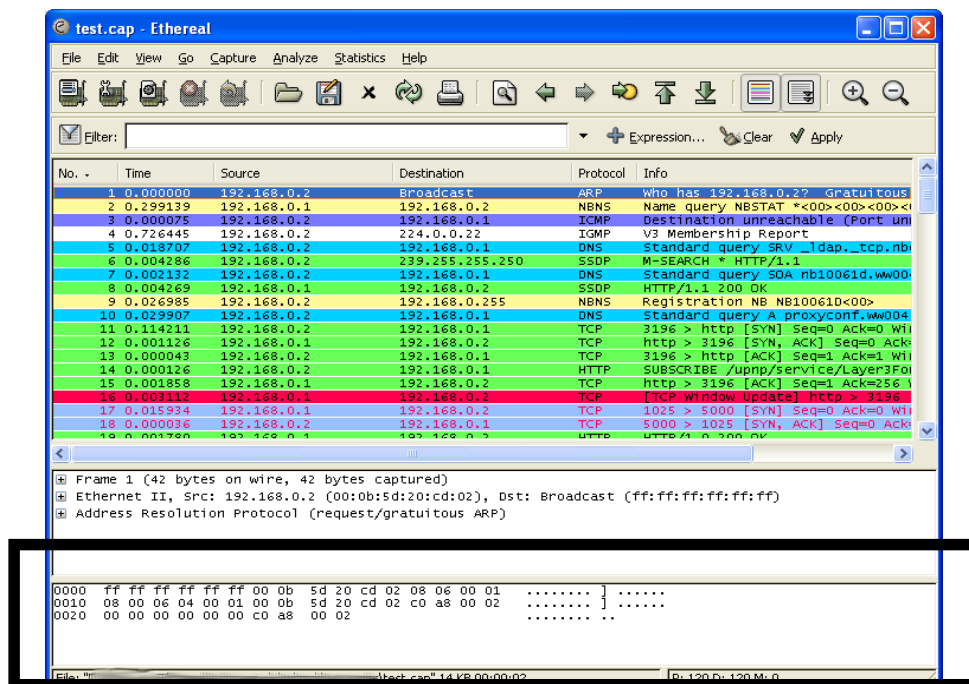
Wireshark Packet List Window

4. Browse the Internet

- Start a capture

- You may combine two filter statements with the ***and*** keyword. Apply a filter to display only ***http*** traffic traveling to or from your ip address. (e.g. If your IP address is 10.10.10.2 enter ***ip.addr == 10.10.10.2 and http***)

- Visit ***http://www.google.com*** and perform a search on ***scurvy***

- Visit the first site in the list

- Return to Wireshark and stop the capture. Analyze the packet data. Was the search word encrypted?

5. View Packet Capture Statistics

- Start a new capture and clear any filters

- Browse the Internet for five minutes

- Stop the capture

- Use the statistics menu to determine the answers to the following questions.
  - How many udp packets did Wireshark capture?
  - What was the average ip packet size?
  - How many packets did Wireshark drop?
  - What does a flow graph show?
  - List the flow graph options.

6. View Packet Header Data

6.1 Capture Packets with Wireshark
4. Start a new capture and clear any filters
5. Browse the Internet for a few minutes
6. Stop the capture

6.2 Explore the Network Interface Layer

6.2.1 Ethernet Frames
- Preamble
  - 64 bits
  - Alternating 1s and 0s, ending with two 0s
  - Used to locate first bit of packet

- Destination Address
  - 48 bits
  - MAC address of recipient

- Source Address
  - 48 bits
  - MAC address of sender

- Field Type
  - 16 bits
  - Identifies higher level protocol

- IP Header

- TCP Header

- Data
  - 46-1500 bytes
  - Information received from Network Layer

- FCS

Preamble	Destination Address	Source Address	Field Type	IP Header	TCP Header	Data	FCS

6.2.2 View Ethernet Frame Data Captured with Wireshark

- Select a TCP packet in the Packet List window

- Expand the *Ethernet* section (Click the + symbol to the left of *Ethernet*.) of the Packet Details window

- Determine the following Ethernet frame values for the selected packet:
  - o Destination MAC Address
  - o Source MAC Address

6.3. Explore the Internet Layer
6.3.1 IPv4 Header: Pictured Below

Version	IHL	Type of Service		Destination Port		
Identification			0	D F	M F	Fragment Offset
Time To Live		Protocol		Header Checksum		
Source IP Address						
Destination IP Address						
Options					Padding	

6.3.2 View IP Header Data for a TCP Packet Captured with Wireshark
- Select a TCP packet in the Packet List window

- Use the Packet Details window to determine the following IP header values for the TCP packet:
    o Version
    o Internet Header Length (IHL)
    o Identification
    o Reserved bit
    o Do not fragment bit
    o More fragments bit
    o Fragment offset
    o Time To Live (TTL)
    o Protocol
    o Checksum
    o Source IP Address
    o Destination IP Address

6.3.3 View IP Header Data for a UDP Packet
- Select a UDP packet in the Packet List window

- Determine values a through m (from step 3.2.2) for the UDP packet

6.3.4 View IP Header Data for an ARP Packet
- Select an ARP packet in the Packet List window

- Use the Packet Details window to determine values a through m for the ARP packet

- Look under Address Resolution Protocol. Determine values for the following fields:
    o Sender MAC Address
    o Sender IP Address
    o Target Mac Address
    o Target IP Address

6.4. Explore the Transport Layer
6.4.1 TCP Header Pictured Below

6.4.2 View TCP Header Data for a TCP Packet Captured with Wireshark
- Select a TCP packet in the Packet List window.

- Use the Packet Details window to determine the following header values for the TCP packet:
    - Source port
    - Destination port
    - Sequence number
    - Header length
    - Window size
    - U bit
    - A bit
    - P bit
    - R bit
    - S bit
    - F bit
    - Checksum

6.4.3 UDP Header Pictured Below

Source Port	Destination Port
Length	Checksum
Data	

6.4.4 View UDP Header Data for a UDP Packet Captured with Wireshark
- Select a UDP packet in the Packet List window.

- Use the Packet Details window to determine the following header values for the UDP packet:
  - Source port
  - Destination port
  - Length
  - Checksum

6.4.5 Compare and Contrast IP, TCP, and UDP
- Do UDP packets have TCP headers?

- Do TCP packets have IP headers?

- What header fields do UDP and TCP have in common?

- Why does TCP have more fields than UDP if they both at the Transport Layer?

- Why don't UDP packets need the *sequence* and *acknowledgment* fields?

- Why don't UDP packets need the *Flag bits* and *Window* fields?

6.5 Explore the Application Layer

6.5.1 Analyze an HTTP Packet

1. Select an HTTP packet in the Packet List window.

2. Summarize the HTTP information available in the Packet Details window. Explain how HTTP uses this information.

3. Does HTTP use UDP at the transport layer? Does it use TCP?

4. Do HTTP packets have IP headers?

5. Draw the HTTP packet. Show the HTTP data, Ethernet frame, IP header, and TCP header. Label the fields in each packet header and fill them with the data obtained with Wireshark.

6.5.2 Analyze a DNS Packet

- Select a DNS packet in the Packet List window.

- View the DNS data information available in the Packet Details window and answer the questions below:
    - What flags do DNS packets have?
    - Is this packet a DNS query or a DNS response?
    - Why do DNS packets have query and answer fields?
    - What is an authoritative nameserver?
    - Does the DNS protocol use TCP at the transport layer? Does it use UDP?
    - Do DNS packets have IP headers?

- Draw the DNS packet. Show the DNS data, Ethernet frame, IP header, and UDP header. Label the fields in each packet header and fill them with the data obtained with Wireshark.

7. Review Questions

- Does Wireshark capture all the traffic on the Internet? If so, explain why. If not, which traffic does it capture?

- Write Wireshark filters to:
  - View udp traffic for 10.10.10.2.
  - View icmp traffic from any address.

- Why don't ARP packets have IP headers?

- Compare and contrast UDP and TCP headers.

- Do ICMP packets specify a port? Look online and explain why or why not.

Cyber Fundamentals #6: The Client-Server Model

1. Introduction
1.1 Exercise Description
Q: What is a secure computer?
A1: An abacus
A2: Unplugged

Functionality and complexity are enemies of security. Generally, the more functionality provided by a system, the harder it is to secure. Servers providing services and opening ports to remote users are particularly prone to vulnerabilities. Attackers often use open ports and exposed programmatic interfaces to subvert a system. This exercise involves reviewing the Client-Server model of computing by installing and utilizing Web, File Transfer Protocol (FTP), and Secure Shell (SSH) clients and servers on Windows and Linux systems.

```
root@ace:~/Desktop# /etc/init.d/ssh start
 * Starting OpenBSD Secure Shell server sshd                    [ OK ]
root@ace:~/Desktop# ssh ace@localhost
ace@localhost's password:
Linux ace 2.6.28-15-generic #49-Ubuntu SMP Tue Aug 18 18:40:08 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/

Last login: Tue Aug 25 09:54:46 2009 from 192.168.2.224
ace@ace:~$ █
```
Starting an ssh server on an Ubuntu localhost and logging in

1.2 Objectives
- Compare and contrast the World Wide Web and the Internet.

- Describe the Client-Server model of computing

- Memorize select server port assignment

- Install and utilize a Web (HTTP) client and Web server
    - Create and serve a simple web page.
    - Analyze HTTP Request and Response Headers with Wireshark

- Install and utilize a SSH client and a SSH server

- Command and control a remote system with SSH

- Install and use an FTP client and a FTP server

- Transfer files with FTP

1.3 Materials
- Computer with access to an account with administrative rights

- VMware Server

- Ubuntu OS iso file

1.4 Assumptions
- The provided instructions were tested on a Ubuntu Jaunty Jackalope image running on a Windows Vista physical machine. Instructions may vary for other OS.

- The student has administrative access to their system and possesses the right to install programs

- The student's computer has Internet access

1.5 Random Notes
- SSH uses public key encryption. Telnet is its unencrypted predecessor.

- Keep in mind there are still many many attacks that compromise encrypted services (ex. video on the sslstrip attack at ***http://www.securitytube.net/Defeating-SSL-using-SSLStrip-%28Marlinspike-Blackhat%29-video.aspx***). With today's technology, no computer or service is 100% secure if it provides any useful functionality!

1.6 Client-Server Model

1.6.1 What is a Server?
A server provides a service and shares its resources (data, computational power) with one or more clients. Examples of web servers include Apache and the Microsoft Internet Information Services (IIS) web server.

1.6.2 What is a Client?
A client requests and/or receives some service from another computing device. Examples of web clients include Firefox and Internet Explorer (IE).

1.6.3 The Client-Server Model of Computing
The Client-Server model of computing involves a service provider (server) and service user (client). If the server is multi-threaded, it can service multiple clients at one time. Examples of applications that utilize the Client-Server model include web, database, FTP, and SSH. For web applications, the server (Apache, IIS) typically listens on port 80 for http or port 443 for https (encrypted). The client (Firefox, IE) forms a Transport Control Protocol (TCP) connection to the server's listening port and requests information (GET http://www.page.com/index.html). The server responds by returning the requested information (index.html) back to the client.

1.6.4 Common Port Numbers
Common services often run on standardized port numbers. See below a list of a few common combinations:
- 20/21 - FTP (data/commands)
- 22 - SSH
- 23 - Telnet (An unencrypted SSH)
- 25 - Simple Mail Transfer Protocol (SMTP - Used by mail servers)
- 80 - Hypertext Transfer Protocol (Unencrypted http web traffic)
- 443 - Hypertext Transfer Protocol over SSL (Encrypted https web traffic)

Keep in mind these are conventions. Nothing prevents administrators from configuring SSH servers from listening on port 20 or web servers from listening on port 5555.
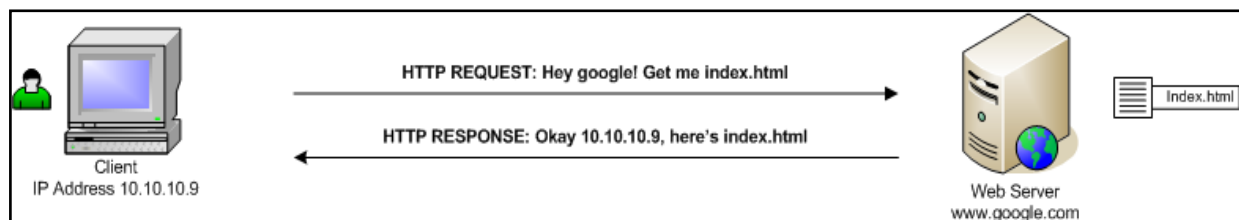
Web client (Firefox, IE browser) requests data (web page index.html)
from a web server (Apache, IIS) listening on a port

1.6.5 Netstat

Network statistics or Netstat is a Windows and Linux command used to view open ports on your system. Open a terminal on either Windows or Ubuntu and type "netstat -an | more" to view active Internet Client-Server connections.

```
root@ace:~# netstat -an | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.168.2.250:44282     64.233.169.103:80       ESTABLISHED
tcp        0      0 192.168.2.250:53707     74.125.127.100:80       ESTABLISHED
tcp        1      0 192.168.2.250:33534     212.58.226.142:80       CLOSE_WAIT
tcp        1      0 192.168.2.250:44552     63.245.209.93:80        CLOSE_WAIT
tcp        1      0 192.168.2.250:44551     63.245.209.93:80        CLOSE_WAIT
tcp        0      0 192.168.2.250:44284     64.233.169.103:80       ESTABLISHED
tcp        0      0 192.168.2.250:41722     74.125.115.102:80       ESTABLISHED
tcp        0      0 192.168.2.250:44281     64.233.169.103:80       ESTABLISHED
```

The netstat command run on a Ubuntu system

Some information gleaned from the screenshot above:

- The system's IP address is 192.168.2.250

- The system is listening on ports 21 and 22.
  What this means: The system may be running an FTP server and an SSH server

- The system is connected to several IP addresses on port 80.
  What this means: The system is running a web browser client and making requests to web servers with the following IP addresses (on port 80)
  - 64.233.169.103
  - 74.125.127.100
  - 212.58.226.142
  - 63.245.209.93

1.7 The Internet and the World Wide Web

The Internet and the World Wide Web are different entities, but people often use the terms interchangeably. The Internet existed before the World Wide Web. Internet-connected computers exchanged email and files long before web browsers, web servers, HTTP, and HTML worked together to make up the World Wide Web. As ***http://www.netlingo.com*** put it "The Web makes the Internet fun to look at and easy to use..."

Internet
- A network of networks
- Made up of computers and cables
- Existed before the World Wide Web
- Uses TCP/IP

WWW
- A layer on top of the Internet
- Made up of web pages, web servers, and web browsers
- Depends on the Internet
- Uses HTTP

1.8 HTML vs HTTP

HyperText Markup Language (HTML) and HyperText Transport Protocol (HTTP) are fancy phrases representing a simple process. Pause and process the individual words in each phrase. HTML is a **language** used to create web pages. HTTP is a communication protocol used to **move HTML** pages from one computer to another. Keep this in mind as you complete the lab.
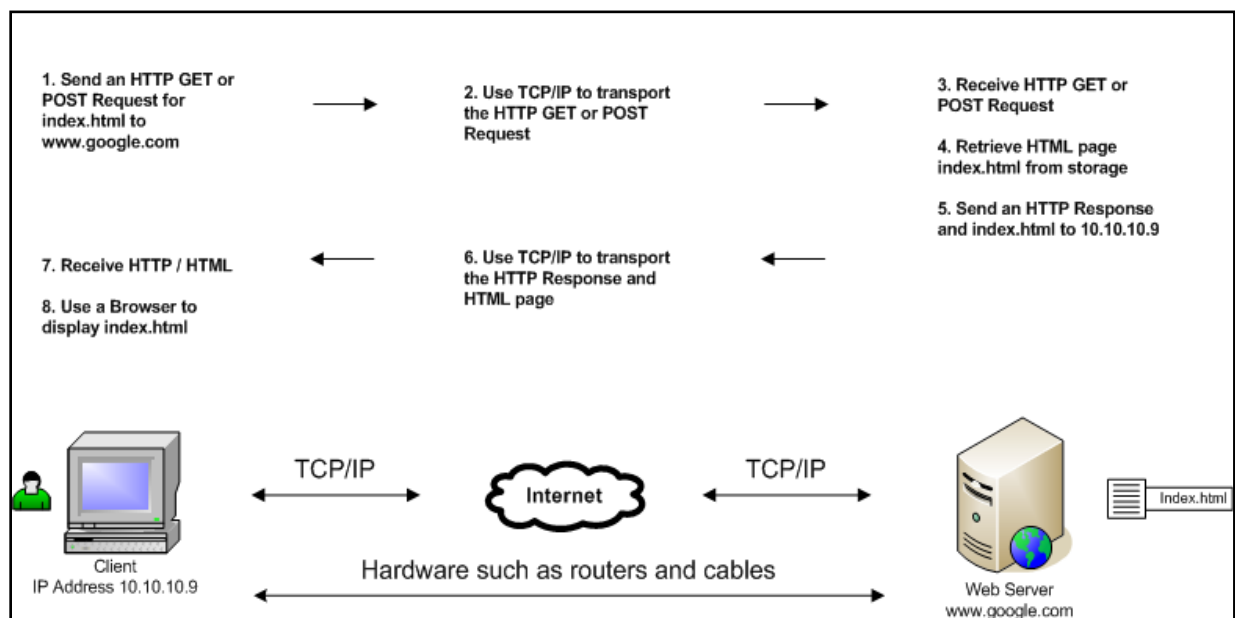
HTTP and HTML

2. Servers and Clients: Web on Windows
2.1 Download and Install Abyss

- Visit *http://www.aprelium.com/abyssws/download.php* and download Abyss.

- Allow the installer to start Abyss when the installation is complete. Follow the instructions and accept defaults.
  - Click *I Agree* for the License Agreement
  - Keep the default for components to install and select *Next*
  - Set the Destination Folder to *C:\Abyss Web Server* and click *Install*.
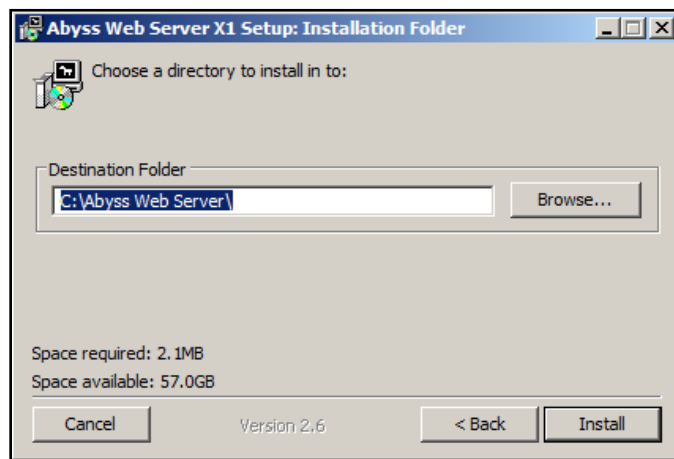
  - Select *Manual startup* and click *OK*
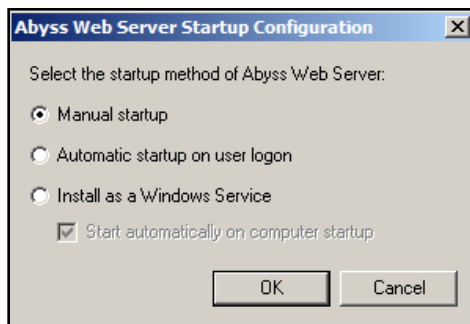
  - Click *Yes* to start Abyss now
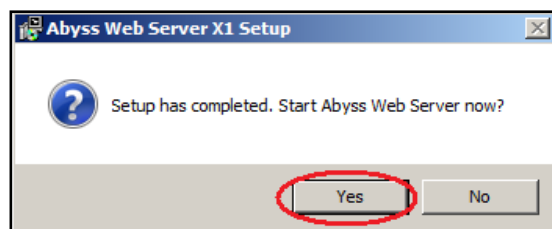
  - Hit *OK* to configure the web server via the web interface.

2.2 Configure the Abyss Web Server

- The Firefox browser should open a web page at *http://127.0.0.1:9999/console/language*

- Select *English*

| English | عربية | Français |
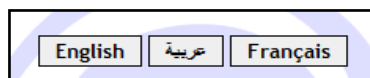
- Enter a login and a password (remember them!) and select *OK*

- Enter the same login and password into the popup box to login to the Server Console
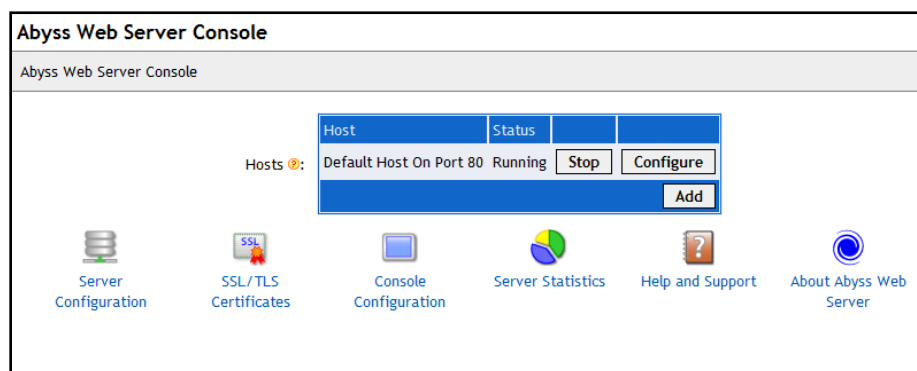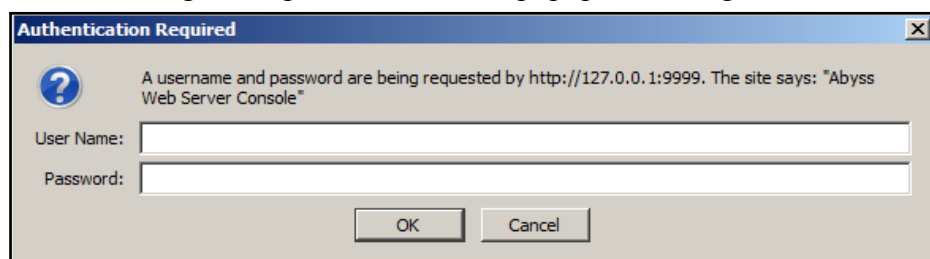
- Note the following:
  - The Abyss web administrative interface runs on port 9999.
  - The Abyss web server runs either on port 80 (default) or 8000 (if something else is already listening on port 80). Remember you can use netstat to view open ports.

- Explore the options provided by the Web Server Console

- Open the windows terminal. Run *netstat -an | more* from the terminal to view that port 80 (or port 8000) is open

- In Firefox, open a new browser tab (*File > New Tab*) and visit *http://127.0.0.1*. You should see a page similar to the image below if the Abyss is up and running.
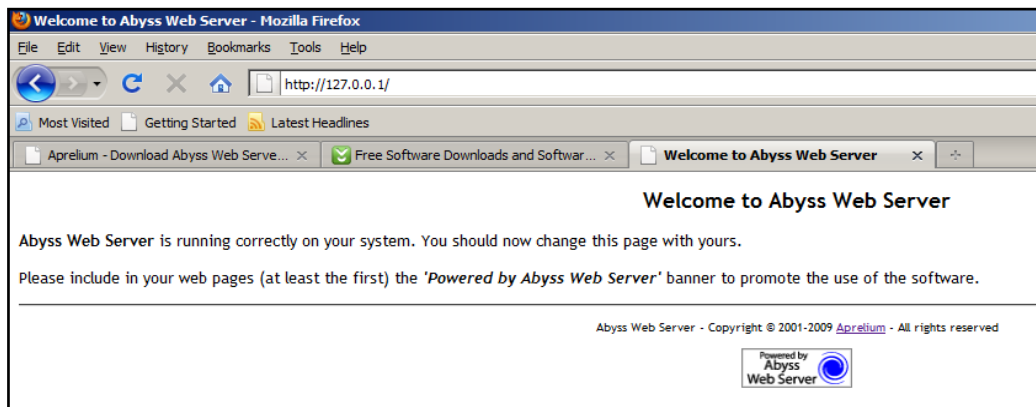
2.3 View Web Page Source Code

- Visit *http://www.securitywizardry.com/radar.htm*

- Right-click on the outer edge of the page (outside any image or box)

- Select View Page Source

- Tags are text strings surrounded by <brackets> that denote the appearance and format of a web page. Locate the following tags in the page source:
  - html
  - head
  - title
  - body
  - img (image tag)
  - a href (link)

2.4 Create a Web Page with HyperText Markup Language (HTML)

- Start a new Notepad document. (Start > All Programs > Accessories > Notepad)

- Type the following into the document:
  <html>
   <head>
    <title>This Might Be My First Webpage </title>
   </head>
   <body>
    <h1> This is the header of my first (maybe) web page. </h1>
    I created this page using HTML.
   </body>
  </html>
- Save the webpage as *index.html* to the Desktop

- Right click *index.html*. Select *Open With > Firefox*

- Personalize the webpage:
  o Set the title to <your name>
  o Change the header and body any way you wish

- View the altered web page with Firefox by hitting the refresh button

- For more information about creating HTML pages visit the http://www.w3schools.com website

2.5 Serve Your Web Page with the Abyss Web Server
- Open Windows Explorer and open *C:\Abyss Web Server\htdocs*

- Replace the Abyss *index.html* with your *index.html*

- Use Firefox to view *http://127.0.0.1* (or *http://127.0.0.1:8000*) and record your observations
  o Note: Any computer may use 127.0.0.1 to refer to itself (can also use *http://localhost*)
  o You can also view by using the internal or external IP address found with the netstat command. (ex. *http://192.168.1.22*)

- Congratuations! You have served your first web page. If you have an externally routable IP address, anyone in the world with an Internet connection and a browser can view it.

2.6 Analyze an HTTP Request Header
- Start Wireshark and begin a live capture

- Apply a filter to ensure Wireshark only displays HTTP traffic leaving from or arriving to your IP address

- Open a browser and visit http://sectools.org/

- Return to Wireshark

- Select the very first HTTP GET / HTTP/1.1 packet originating from your IP address. Use the Packet Details Window to answer the following questions:
  o What is the request method?
  o What is the request URI?
  o What is the request version?

- Why is there more than one HTTP GET request? What are the other requests asking for?
- Examine the Packet Details Window and find the values of the HTTP Request Headers (some fields may NOT be present, don't worry about it!)

- o Host
- o User-Agent
- o Accept
- o Accept-Encoding
- o Accept-Charset
- o Keep-Alive
- o Connection
- o If-Modified-Since
- o If-None-Match

2.7 Analyze an HTTP Response Header
- Select the first HTTP/1.1 200 OK (text/html) packet sent back to your IP address. Record the response code returned by the server.

- Examine the Packet Details Window and find the values of the HTTP Response Headers (if present)
  - o Date
  - o Server
  - o Connection
  - o Keep-Alive
  - o Accept-Ranges
  - o Content-Length
  - o Connection
  - o Content-Type

- Look at the Individual Packet Bytes window. What kind of data does it contain?

2.8 View HTTP Packet Data
- Examine the packet data of several HTTP packets with an Info field of HTTP/1.1 200 OK(text/html)

- Find a packet which has an Uncompressed entity body tag at the bottom of the packet data window

- Select the Uncompressed entity body tag to view the uncompressed html

- Describe the information available under this tag

3. Servers and Clients: Secure Shell (SSH) on Linux

3.1 Introduction
SSH enables C3 (Command, Control, and Communication) of a remote system, by giving a user a terminal for the remote system. It also enables transferring files using the scp command. In this section you'll accomplish the following objectives:

- Windows
    - Download and setup freeSSHd server
    - Download and utilize the SSH PuTTY client

- Linux
    - Install the Linux Open-SSH server
    - Use the Linux Open-SSH client
    - Practice issuing remote commands

3.2 Download and Install an SSH Server on Windows

3.2.1 Download and Install freeSSHd
- Download the latest version of *freeSSHd* from *http://www.freesshd.com/*

- Double click the freeSSHd.exe to begin installation and select *Run*

- Accept all of the defaults and click *Install*

- Select *Yes* to create private keys

- Select *No* to run as a system service

- Select *Finish*

3.2.2 Start freeSSHd

- Double click the freeSSHd shortcut icon on the Desktop

- In the taskbar (bottom right-hand side of screen), right click the ssh icon and select *Settings* to open the configuration screen
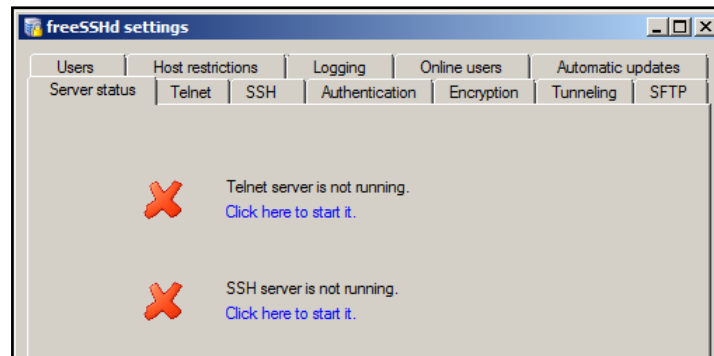
Configuration screen for free SSHd

- Select the *Users* tab and click *Add*

- Add a *login* name of *win*, select *Password stored as SHA1 hash*, enter the *password ilikewin*, and select the functions the *user can use* and select *OK*
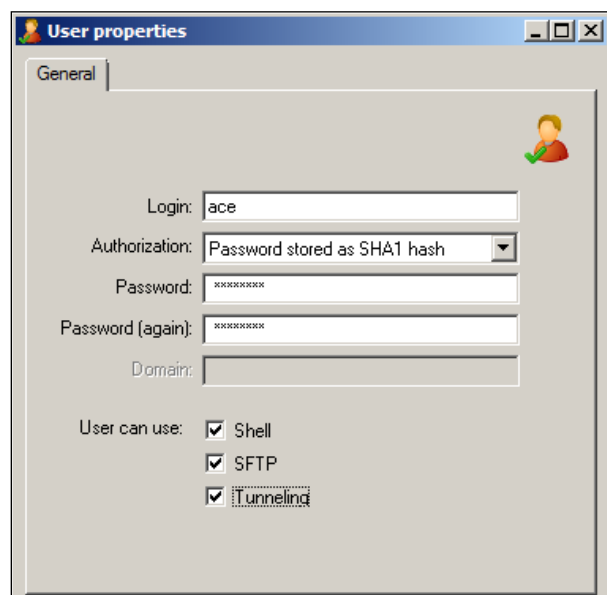
- Select the *Server Status* tab

- Click to start the SSH server

- Open a terminal and run *netstat -an | more*. Note that the SSH server is now listening on port 22.

3.3 Download and Run an SSH Client for Windows

- **Disable Firewall:** If you are using Windows Vista or Windows XP:
  - Go to *Start > Control Panel > Classic View > Turn Firewall On/Off*
  - Turn the *Firewall Off*

- **Disable User Access Control:** If you use Windows Vista also:
  - Click *Start*
  - In the Search Bar type *MSCONFIG*
  - Select the *Tools* tab
  - Scroll down to *Disable UAC*
  - Restart computer

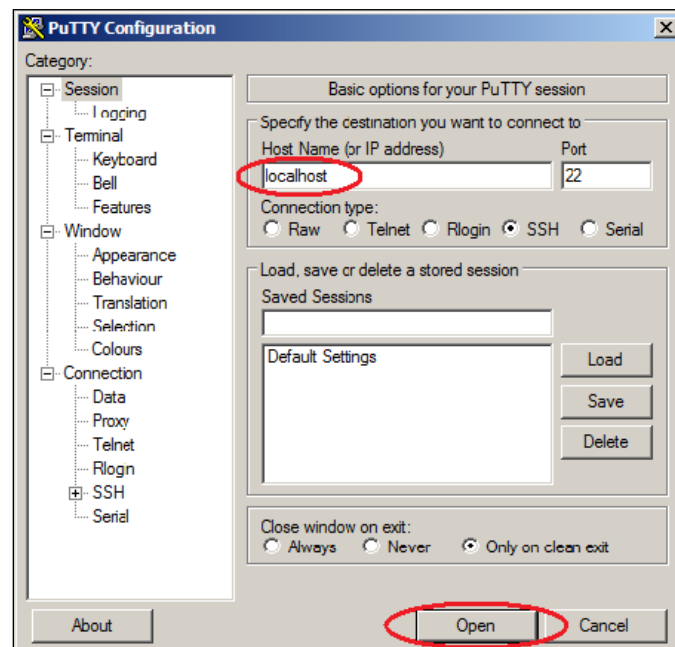- Visit http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

- Download *putty.exe* for Windows and double-click the file to start PuTTY

- Enter *localhost* or *127.0.0.1* (both refer to your local computer, or your could enter your host's external IP address) under Host Name and click on *Open*

- Click *Yes* when you get the Security Alert

- Enter the user name and password you specified to get terminal access via SSH

- Close the PuTTY window
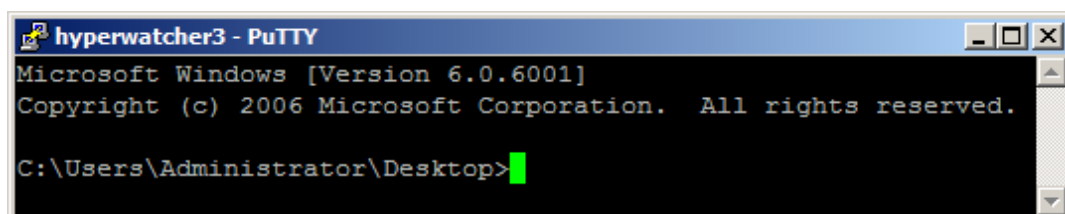
3.4 Download and Install an SSH Server on Linux
3.4.1 Download and Install openssh
- Install the *openssh-server* package on your Linux Image (with Synaptic Package Manager or apt-get)

- Open a terminal
  - *netstat -an | more*   //Note that port 22 is listening
  - *ssh ace@localhost***   //Log into the openssh server with the ace account
  - Enter *yes* to the security warning
  - Enter your password
  - To quit, type *exit*

(**Note: The Ubuntu OS has an ssh client installed by default)

3.4.2 Configure openssh
Open a terminal
- *sudo -s*   //Escalate privileges
- *cd /etc/ssh*   //Remember the /etc directory holds configuration info
- *cp sshd_config sshd_config~*   //Make a backup of the openssh server configuration file
- *gedit sshd_config*   //Open the openssh server configuration file for editing

Review the ssh server configuration file. Change the listening port from 22 to 333. Save the file and exit.
- */etc/init.d/ssh restart*   //Restart the server to load the configuration changes
- *netstat -an*   //Note that port 22 is closed, port 333 is listening
- *ssh ace@localhost*   //This will fail, we need to tell the ssh client to use 333
- *ssh -p 333 ace@localhost*   //Login on port 333
- *exit*
- *cp sshd_config~ sshd_config*   //Copy backup file over changed file to change listening port back to 22
- */etc/init.d/ssh restart*   //Restart the server to load the configuration changes

3.4.3 Stop, Start, and Restart Servers (like openssh)
Open a terminal
sudo -s
cd /etc/init.d/   //The init.d directory contains start, stop, and restart scripts
ls   //Review the different services that have init.d scripts
/etc/init.d/ssh stop   //Stop openssh server
/etc/init.d/ssh start   //Start openssh server
/etc/init.d/ssh restart   //Restart openssh server

**Note that these changes are typically temporary. For example, if you stop the openssh server and restart the system it will automatically start unless disabled (see 3.2.2)

3.4.4 Enable and Disable openssh
- From the Ubuntu GUI go to *System > Administration > Services*
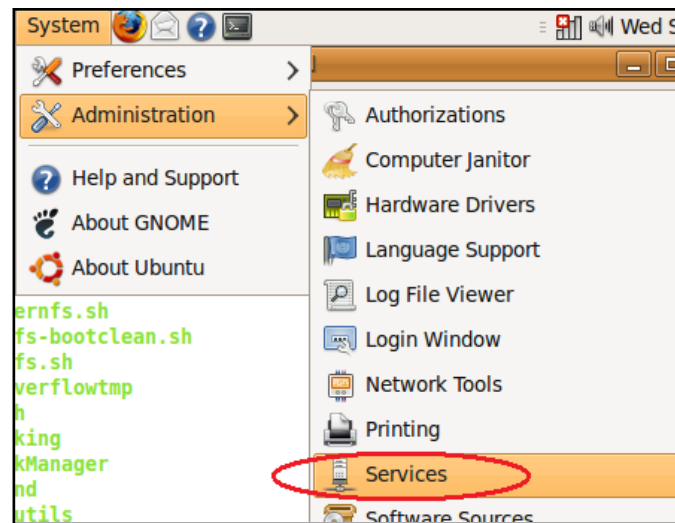
- Click *Unlock* and enter the password

- To disable a service, uncheck the associated box. To enable, check the box.

3.5 Issue Commands to a Remote System

3.5.1 Reminder: HOWTO Determine IP Addresses
- On Linux open a terminal and type *ifconfig* (interface is typically eth0 or eth1)

- On Windows open a terminal and type *ipconfig* (interface is typically Local Area Connection)

3.5.2 ssh into Windows from Linux
- Open a Linux terminal

- Type *ssh win@<windows ip address>*

- Enter the password

- Voila – you have a Windows-like terminal into the Windows system

3.5.3 ssh into Linux from Windows
- Open PuTTY

- Enter the Linux IP Address and click *Open*

- Enter username *ace* and password *ilikeace*

4. Servers and Clients: FTP on Linux

- Install the *vsftpd* package on your Linux Image (Synaptic Package Manager or apt-get)
- Open a terminal

cd ~	//Move to your home directory
*netstat -an	more*	//Note that port 21 is listening
echo hi > sample.txt	//Create a file named sample.txt
ftp localhost	//Log into the openssh server with the ace account

Enter user name and password

pwd	//List the present working directory
dir	//List contents of directory
help	//View available commands
put sample.txt	//Upload sample.txt to the server (really the same computer since using local host!)

Open a new tab on the terminal

cd ~	//Move to your home directory
rm sample.txt	//Delete sample.txt on your local computer
	Return to tab with ftp session
get sample.txt	//Download sample.txt from the server
exit	//End your session

5. Review Questions

6. You used Firefox (or IE) and Abyss. Identify the client and the server.

7. Can a single computer act as a web client (browser) and a web server at the same time?

8. With the proper software, can any typical Internet-connected, functional computer serve web pages?

9. Can the HyperText Transport Protocol transport anything besides HyperText Markup Language?

10. You run netstat from the terminal and notice that an application is listening on port 80. Does this indicate a web server running on the machine?